Section C – Statement of Work

Executive Summary

The Department of Defense (DoD) Civilian Personnel Management Service (CPMS) has developed and deployed the Defense Civilian Personnel Data System (DCPDS), the Department's enterprise civilian human resources (HR) information management and transaction processing system supporting over 800,000 DoD civilian employee records and 1.5 million position records. DCPDS supports appropriated and non-appropriated fund (NAF) employees, as well as local national and National Guard Bureau (NGB) personnel through 22 DoD Regional Service Centers (RSC) and over 300 Customer Support Units (CSU) worldwide. System upgrades and enhancements to DCPDS continue as an organized, coordinated activity centrally managed by CPMS.

DCPDS was designed to improve and simplify personnel transaction processing, the delivery of personnel services, and retrieval of timely civilian workforce information. CPMS is responsible for functional and technical oversight of DCPDS. Deployment of the system began in October 1999, reaching Full Operating Capability (FOC) in September 2002. CPMS managed DCPDS development and deployment, and currently administers the operation, maintenance, and sustainment of DCPDS through a commercial contract. In July 2003 the migration of DCPDS from a client-server to a web-based environment upgraded the application software to the newest release.

DCPDS uses a Commercial Off-The-Shelf (COTS) product (Oracle HR), customized for the Federal and Defense environments, to provide personnel transaction processing using Oracle Federal HR. Resumix (Yahoo Corporation), another COTS product, has supported an automated recruitment and staffing process. In addition to COTS software, CPMS developed customized code to support 12 demonstration projects, 11 unique local national applications to support requirements for 17 countries, NAF employees, and NGB employees. Other application developed by CPMS and incorporated into DCPDS include: COREDOC, used to support the classification and position description processes; AutoRIF (interfaced to DCPDS), used for reduction-in-force; a CSU application for standard report and retrieval; and productivity, used to track the status and timeliness of personnel action processing. DCPDS operates on a Hewlett Packard (HP) UNIX platform.

DCPDS provides personnel transaction and employee information capability at DoD regional service centers (RSCs). Corporate information supports strategic decision-making. The Corporate Management Information System (CMIS) provides consolidated information covering over 800,000 DoD employees on a single server. Under the CMIS-Revised (CMIS-R) project, begun in 2004, the update process, accessibility by DoD managers, and accuracy of DCPDS corporate data will be greatly improved and enhanced. DCPDS interacts with other information systems by interface or direct data feed, most importantly as the HR data interface with the Defense Civilian Pay System (DCPS). DCPDS provides civilian personnel management information down to the desktop of managers and supervisors. Contract support must provide system operation, maintenance, and sustainment, including applicable database administration, systems administration, and hardware operations, to support system usage via a server network that is distributed worldwide. This support must include development, testing and communication server requirements as well. In addition, separate contractor support will be required for additional development work over the life of the contract. These requirements are delineated in detail in the Statement Of Work (SOW).

The Department has been authorized to establish a new HR management system for its more than 800,000 civilians – the National Security Personnel System (NSPS). Changes to DCPDS will be required to accommodate new rules, regulations, and processes based on the design of NSPS. The requirements for DCPDS system changes will be reflected in a separately priced Contract Line Item Number (CLIN) as the functional requirements are defined by the Government. The CLIN will address the software development and configuration management effort of the contractor based on a time and materials basis. Details of this requirement are in section C.3.5.1.

The basic period of performance for this contract is five years (base year plus four option years), beginning from contract award. The Government expects that under the terms and conditions of the SOW the contractor will perform as a full business partner. Open and direct communication is expected at the executive, program management and action officer level. Issues will be cooperatively addressed and resolved. Any dispute will be addressed at the lowest possible level and worked to resolution using contract provisions and proper acquisition oversight.

C.1. Overview

C.1.1. CPMS Overview

CPMS is responsible for operation of consolidated civilian personnel programs and services for the entire Department. The primary customers are approximately 7,500 civilian personnel specialists at the component (Army, Air Force, Navy and each of the Defense Agencies) headquarters, major commands, and field operating levels. DCPDS also supports the Executive Office of the President and the Broadcasting Board of Governors/International Broadcasting Bureau (BBG/IBB).

CPMS is part of the Defense Human Resources Activity, an Office of the Secretary of Defense field operating activity, under the direct control of the Under Secretary of Defense for Personnel and Readiness. The CPMS Regionalization and Systems Modernization Division, System Management and Program Administration (SM/PA) Branch, will administer the resulting contract. The SM/PA Branch supports the program management efforts of the CPMS Director and the Chief of Regionalization and Systems Modernization Division by providing acquisition program management advice and assistance, and technical guidance on the operation, maintenance, and sustainment of DPCDS. Business reengineering support and functional guidance are the responsibilities of the Plans and Programs Branch and the Functional Requirements, Testing and Operations Branch. The SM/PA Branch provides management oversight and support to procurement, contract, and certification activities; exercises program management responsibilities regarding vendors that support DCPDS; and coordinates the support relationships between CPMS, its customers, and system vendors.

The DCPDS program manager, Deputy Director for HR Automated Systems, is responsible for directing DCPDS program efforts, including communications with Components and the contractor. For additional information on CPMS, refer to the CPMS home page located at ***www.cpms.osd.mil***. Through this contract, CPMS intends to obtain turnkey contractor support for the operations, maintenance, and sustainment of DCPDS. The contractor must use the commercial best practices of the industry to perform work under the resulting contract.

C.1.2. DoD Customer Overview

DoD has centralized many of the HR functions into RSCs; the decentralized functions are performed in the CSUs; and each RSC supports multiple CSUs. DoD has a total of 22 RSCs and over 300 CSUs (a detailed listing is at Attachment 1). Also referenced in this document are CSU databases. There are only 24 CSU databases because most Components have centralized groups of CSUs into one database. Throughout this document, reference to Customer Support Unit will be shown "CSU"; reference to the database or server will be shown as CSU "databases".

C.1.3. Non-DoD Customer Overview

CPMS currently provides DCPDS support to two non-DoD customers. They are the Executive Office of the President, and the BBG/IBB. They are provided full coverage under this contract (also shown in Attachment 1).

C.1.4. DCPDS Overview

DCPDS is a multi-function, civilian HR information management and transaction processing system. The system supports over 800,000 current civilian employee records (appropriated fund, non-appropriated fund, National Guard Bureau, and local nationals) and 1.5 million position records, with approximately 7,500 civilian HR specialist users. The serviced population could increase to as many as 850,000 employees. It is a global system supporting users in Asia, Pacific, Europe and North America on a 24 hour, 7 day a week basis (approximately 15% of users are located in Asia, Pacific, and Europe).

The system uses standard communication protocols over the Defense Information System Network (DISN), which is maintained by the Defense Information Systems Agency (DISA), and applications operating against distributed databases. The DISN supports communications: base-to-base, base-to-hub, and between RSCs and CSUs.

COTS products (Oracle HR Federal, and Resumix) are the core of DCPDS. A complete listing of all applications that make up the DCPDS can be found in section C.3.

DCPDS operates with 17 DoD RSC servers, a DoD corporate management information system (CMIS/CMIS-R) with a suite of three servers, and a DoD training and demonstration server (up to three instances). The system also includes up to 24 CSU databases (a detailed listing is at Attachment 2).

C.1.5. Contract Overview

CPMS has established limited, focused performance metrics. The metrics will be used to evaluate the contractor's job performance. The contractor will collect metric data, normally through an automated method, to facilitate this evaluation. The contractor will be required to provide specific reports required by this contract and will provide copies of all such reports to the CPMS Contracting Officer's Technical Representative (COTR). This SOW describes the requirements for ongoing operation, maintenance and sustainment support of DCPDS. This SOW frequently uses the term "days" as a measurement. In all such cases, it is the Government's intent that these are calendar days and not business days.

C.2. General Specifications Guiding Statement of Work Preparation

This SOW has been prepared with the best information available to CPMS. In several cases the Government has projected September 2005 requirements. Software versions reflected are the ones that will have been developed, tested, and deployed by that date. The contractor will work with the Government in handling unforeseen changes, such as the issuance of new Oracle or Resumix software versions. Hardware configurations also have been projected and these may change as technological advances occur.

C.3. Contract Scope

C.3.1. DCPDS Concept of Operations (CONOPS)

The following CONOPS description is provided to assist the contractor in identifying the scope of its responsibilities as follows:

- Data flow describes the flow of information between servers and the various users.
- Operation, maintenance and sustainment of DCPDS describe the basic services and support provided by the contractor as delineated in section C.3.1.2.
- Program and project management describe the roles of CPMS staff in the overall coordination and management of DCPDS.

C.3.1.1 Data Flow

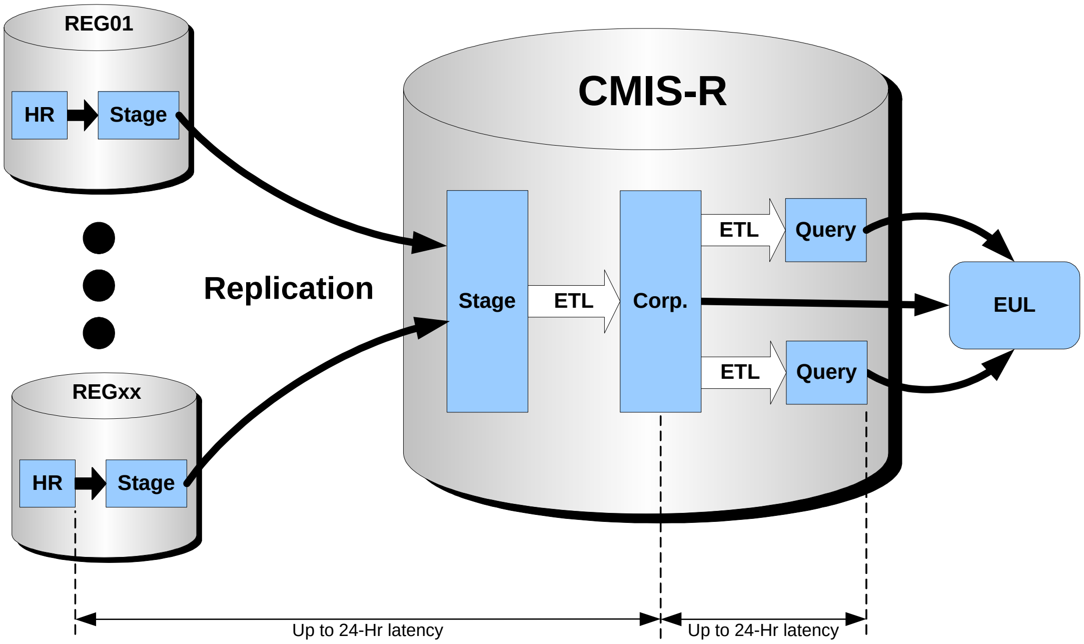
DCPDS exists at three discrete levels:

- CMIS database residing at the contractor-provided facility;
- RSC servers and a training and demonstration server (see Attachment 3 for a detailed listing of server locations); and
- CSUs (residing on the HR application, except Air Force).

Users access the RSC servers to accomplish all transaction-level processing. Information from RSC servers is downloaded nightly to each CSU within the RSC. Users normally use the CSUs for running queries and reports. RSC and CSU personnel staffs may run queries and reports against the RSC server.

In addition, transactions from the RSC servers flow to the CMIS database on a continuous basis. This current transaction forwarding is accomplished using the Data Transfer System (DTS), which is a DoD-developed solution. Currently, the contractor is responsible for maintaining the DTS code.

CMIS-Revised (CMIS-R) is scheduled for deployment in May 2005. Included in this revision is a replacement update process for DTS. The DTS function does not provide the database integrity required for corporate reporting requirements. The current CMIS contains inaccurate information, requires long-running refreshes, and the data is untimely. Inaccuracy is caused by the transactional nature of CMIS HR; DTS processing; edits and business rules invoked at CMIS; Oracle patch problems at CMIS HR; errors from the manual recovery process, and DTS downtime. As part of the CMIS-R project, the current DTS process will be replaced by an extraction, transformation, and loading (ETL) process. The ETL process will move data between the CMIS-R staging area, the data warehouse, and six (6) additional data marts, each of which may be accessed by one or more metadata layers. The contractor will be responsible for maintaining the code that supports the ETL process.



Wide Area Network (WAN) connections are provided through the DISA DISN. Local Area Networks (LANs) are provided for each CSU and RSC and are the responsibility of the components and other Federal agencies. Connections from the contractor’s hubs to the Non-

Classified Internet Protocol Router Network (NIPRNET) are jointly arranged, and are at Government expense.

C.3.1.2. Operation, Maintenance, and Sustainment of DCPDS

CPMS will be responsible for DoD business activities (policy and functional support) and program management. CPMS will be responsible for necessary coordination with Components or other Federal Agencies that use or may use DCPDS. The Contractor is responsible for providing all personnel, material, and resources, except as otherwise set forth in this contract, for the operation, maintenance, and sustainment of DCPDS. In performance of the tasks described below, the contractor shall adhere to approved Federal and DoD IT architectures, guidelines, and standards, as referenced in the DoD instructional guides.

- Help Desk Support. The contractor shall provide 24-hour by 7-day (24 x 7) technical help desk support to CPMS, component and Agency first-level help desks. The contractor shall provide at least 12-hour by 5-day (12 x 5) functional help desk support (6am to 6pm Central Time, Monday through Friday). The functional help desk provides detailed processing assistance for use of the system and is to be staffed by individuals who have developer level knowledge of the system.

- Database Administration. This consists of basic and advanced technical activities associated with the effective and efficient operation of DCPDS.

- Systems Administration Support. Systems administration consists of daily operations maintenance, outage and problem response, systems performance, user access, user information, and security of DCPDS.

- Application Sustainment and Maintenance. This service includes the activities associated with maintaining the functionality and proper configuration of DCPDS.

- Technology Refresh. The contractor will provide technical support, guidance, and planning support for these activities. The contractor shall be required to serve as the technical expert for the total system. CPMS will look to the contractor as its technical advisor on the system, to include review of requested configuration or equipment changes and to recommend needed technology changes during the life of the contract.

- Information Assurance Officer (IAO). The contractor will establish a security unit headed by a certified Information System Security Officer (ISSO) as described in section C.8.

A prime area of emphasis across the operation, maintenance, and sustainment of DCPDS has been rigorous Configuration Management (CM) processes. DCPDS requires a disciplined CM process because of the dynamic nature and complexity of the software development and patch process, including fielding repairs to problem reports, adding new system changes, and normal software maintenance. The support CM processes used to operate, maintain, and sustain DCPDS have focused on process improvement, resulting in actions taken, by both CPMS and the system integrator, to continuously improve the CM process. The CM processes are based on:

- Addressing systemic causes, not the symptoms, through root cause analysis;
- Minimizing latent defects through developmental peer reviews;
- Ensuring correct and timely distribution of patches by isolation of production patch files and automated control of the patch windows;
- Continuing improvements of pre-application review checklists and hosting meetings to discuss unique situations or deviations for a particular patch (i.e., communications outages, etc);
- Initiating process changes in code audits to ensure baseline compliance;
- Using Serena^{TM} Version Manager^{TM} tool header and file naming convention to improve identification;
- Increasing depth of review of Oracle patches, including comparison of the data before and after the application of patches; and
- Using tools such as Integra^{TM} Code Base for automated review of code changes.

These process improvements have resulted in a steady decrease in new DCPDS problem reports. The contractor will continue this rigor in CM processes.

C.3.1.2.1. Help Desk Support

Three levels of help desk support will be available to DCPDS users.

- Level 1. Component-Level Help Desk.
  If a user encounters a problem, there are two tiers of immediate support provided by the Government.

  Tier 1A is local-level or desk-side support. This service is the first point of contact for users and provides the first opportunity to address a problem, regardless of the technology or nature of the problem. This support is provided at the CSU or RSC by component staff.

  Tier 1B support occurs at the component or agency level by a component support desk. Any issues or problems that cannot be solved by Tier 1A staffs are escalated to component staff for resolution. Trouble ticket reporting is done only from this tier level. Reporting is done only after the problem is researched, documented, and confirmed. Because of their size or RSC approach, some components only provide Tier 1B help desk support.

- Level 2. Contractor Help Desk (staffed and equipped by contractor at a contractor facility). Should a problem or issue be "irresolvable" through the Level 1 help desk, the problem will be escalated by the Tier 1B component support personnel to the Level 2 contractor help desk. The contractor help desk will be operational 365 days per year, at a facility provided by the contractor. The contractor shall track all Level 2 help desk calls until the problems are resolved. The contractor shall enter all calls, including those resolved by Level 2 help desk personnel into a tracking system maintained by the contractor. All hardware problems on component Government Furnished Equipment (GFE) are dispatched to the component help desk staff for dispatch and resolution, with notification to CPMS technical staff. All HR policy and procedure questions are escalated to CPMS system development team. All incoming calls and responses will be in English. The contractor shall staff the Level 2 help desk with individuals knowledgeable of the HP UNIX hardware and operating system environment, Oracle DataBase Management System (DBMS), Resumix, Oracle HR, and any other software used in conjunction with DCPDS. Responses will be responsive, timely, and accurate and will be provided in clear and effective English.

- Level 3. Dispatch and Tracking of Third Party Support or Contractor Experts (staffed and equipped by the contractor at the contractor facility). The contractor shall enter all calls, including those resolved by Level 2 help desk personnel, into a tracking system, maintained by the contractor. Should a problem arise that cannot be resolved by the Level 2 help desk, the contractor remains ultimately responsible for the resolution of that problem. The contractor is responsible for escalating problems to other third parties, such as Oracle, Resumix or HP, as required. If necessary, the contractor is responsible for providing the expertise internally. When the problem is based on GFE, the contractor refers the problem back to the owning component and notifies the CPMS technical staff, or notifies CPMS directly, as appropriate. Service level expectations are suspended on that RSC server until the component resolves the problem. If the problem is with CFE, the contractor will track the problem and report its status and resolution to CPMS.

The contractor will also provide, as a deliverable, a monthly report on all calls that are received (Call Detail Reports – CDRs), including analysis of common causes and problems, capacity constraints, requirements for preventive maintenance and upgrades, trend analysis, user training deficiencies, and other common issues. This report shall include a list of CDRs that are open at the end of the calendar month, the history of the CDR since creation, and the current owner of the call. These reports shall be provided to the COTR no later than the 10th day of the month following the previous month report period. Reports may be in electronic format. Should any unique software be necessary to read or evaluate the report, the contractor shall provide the software to the COTR.

CPMS and the components are responsible for GFE hardware warranty and maintenance costs.

The contractor shall have a single worldwide phone number for all incoming help desk calls. The contractor shall provide this toll free number as CFE. The contractor help desk tracking system shall be able to report such calls with differentiation of the purpose of the call. Normally, this will allow the report to indicate the number of calls received, not to include callbacks or contractor staff use of the system.

The contractor help desk is not normally expected to speak with an end-user, unless a specific problem requires user input. All incoming help desk calls should come from the component or agency help desk. CPMS will provide a list of authorized personnel who may contact the contractor help desk; only calls from authorized individuals will be accepted. Other calls are to be referred to the component's tier 1B help desk. When the contractor help desk needs additional information, it contacts the component help desk. In rare cases, the contractor provided help desk will call the system end user directly.

C.3.1.2.2. Database Administration

The contractor provides database administration for the CMIS/CMIS-R database, all RSC servers, and all CSUs. Database administration activities are performed centrally from the contractor's site. Database administration facility(ies) are contractor provided and the number and location of these facilities are at the discretion of the contractor. Database administration includes all physical and logical data management (such as daily monitoring and correction of errors that fall out at the CMIS/CMIS-R level). Physical loading of backup tapes and on-site tape library management are not database administration; these duties are considered systems administration.

Database administration activities include, at a minimum, data integrity maintenance, data backup and recovery, configuration management, database performance tuning, physical and logical database support, and support for database changes and upgrades. Database administration also includes reacting to and correcting DBMS- related outages or other reductions in service.

Personal Computer (PC) and LAN databases will be maintained by component personnel and are outside the scope of the contractor.

C.3.1.2.3. Systems Administration

The contractor is required to provide technical evaluation of systems hardware/software and recommend changes as required to ensure the most effective and efficient system is implemented.

The contractor will provide systems administration services for the CMIS/CMIS-R database, all RSC servers, to include Resumix servers, and the training and demonstration servers at CPMS in Rosslyn. The duties to be performed under the area of systems administration are reflected in Attachment 4.

Systems administration consists of daily operations, maintenance, systems performance, user access, user information, and security of DCPDS (as referenced in section C.3). This includes loading backup and other tapes, assisting in system audits, tuning of the system, managing the operating system for optimum computing performance, and performing other daily operational tasks. Systems administration also includes reacting to and correcting system outages or service degradations. Problems with any service degradation issues related to hardware, operating system, networks, and any other system software tools remain a system administration oversight responsibility until the problem is corrected.

Systems administration also includes the following activities:

- Data backup and offsite storage, including nightly incremental backup of each RSC server and the CMIS/CMIS-R database, with full volume backups taken each week. Data is then sent offsite to be used in the event of a disaster.
- Continuity Of Operations Plan (COOP) and disaster recovery that includes support for the component's restoration activities for RSC servers at the time of disaster. COOP support for RSC servers may require the contractor to provide support at an alternate location or immediate coverage for a systems administrator who is incapacitated. The contractor may be required to provide a current ignite tape for some COOP efforts. For the CMIS/CMIS-R database, it includes all strategy development, hot-site fees, planning, and execution support for recovery. Recovery shall begin within 24 hours and be completed within five calendar days. The CMIS/CMIS-R COOP shall be tested at least annually, with CPMS involvement.
- Tape library management that includes the storage and management of tapes, disks, and other magnetic media. Media storage will occur at the RSCs, at the contractor location(s), and in third-party offsite storage facilities. The contractor will be responsible for administering the locations of such storage.
- Electronic data interchange within DoD or with external Government agencies, which includes receiving data and loading it into the system and exporting data and sending it out to other Government agencies. Currently this involves flat files, but could include relational database transfers in the future. The existing flat files have set layouts that may be modified as necessary. These files are both outgoing and incoming.
- Production control including scheduling, monitoring and ensuring successful completion of all batch and online transactions.
- Change control including documenting, scheduling, testing and implementing all changes to the production environment, including hardware, software and network modifications. The contractor will plan for roll back procedures for major modifications. This also includes the development and test environment supplied by the contractor as CFE.
- Capacity planning including a monthly report by the contractor. The monthly report to CPMS will document any situation where increases in processing or communications capabilities are required for the continued or optimum operation of the system. The contractor shall be involved in all capacity planning exercises that the Government sponsors related to DCPDS. For planning purposes this is expected to occur twice during the contract period and require at least three contractor personnel and equipment as required over a three-week period. Under the technical refresh role, the contractor may recommend capacity-planning exercises.
- Automated and manual performance monitoring and the collection and reporting of required systems performance metrics. The contractor will provide an automated tool to perform system monitoring. The Government will work with the contractor to resolve connectivity (firewall) problems; however, such problems will not excuse the contractor from providing

automated monitoring. Should added equipment be necessary to comply with access rules, it will be at contractor's expense. This expense shall be limited to no more than $3,500 per RSC during the life of the contract; anything over that amount will be negotiated with the Government, normally on a shared cost basis. The contractor will be required to report some of the performance metrics on a daily basis and others on a monthly basis, as jointly defined by CPMS and the contractor after contract award.

- Systems management, including all activities to keep the systems operating at peak performance with minimal downtime. It includes reacting to and correcting outages and downtime.
- Dispatch and tracking of remote support personnel (warranty/maintenance provider, on-site systems administrator, etc.).
- Technical evaluation of systems hardware/software and proposed changes.

A contractor shall develop an operations manual for system administrators within six months of contract award. The manual will include standard operating procedures and emergency procedures that are specific to this environment as well as the actual detailed steps and procedures to be used by the system administrators. CPMS recognizes this manual as the property of the contractor; it will not be shared with external third parties. Use of the manual is intended for the Governments use.

The locations of the RSC servers are at the discretion of the Government. The Navy's centralized service center in Jacksonville, FL, is supported by DISA, which provides support for seven of the eight Navy RSC servers. (Navy Europe is supported from the United Kingdom.) The location of all RSC servers is at Attachment 1.

The majority of the Systems Administrator (SA) duties in this SOW can be performed centrally. However, at least one SA shall be co-located at the Army RSC, the Air Force RSC, the Navy's consolidated operations center in Jacksonville, FL, any future consolidated service center, and at each RSC outside the Continental United States (currently Army locations in Korea, Germany and Alaska). The contractor may need to provide multiple administrators at some sites in order to provide systems administration support to ensure optimum operation of the system. The contractor is also responsible for providing limited SA support at the CPMS site at Randolph AFB in San Antonio. While there is no server located at this location, the SA will be required to provide support to include loading patches and trouble-shooting software (such as DCPDS, Business Objects, Test Director, Remedy, Ghostview, CSU database, or other similar applications).

The contractor may choose to provide systems administration support either on-site at the remaining RSCs or by remote centralized support. Regardless, the contractor remains responsible for all of the systems administration duties shown at Attachment 4. In its proposal, the vendor is responsible for outlining how it will provide systems administration and how it will cover short-term absences of SAs during periods of vacation, illness, training or departure. It is inevitable that these employees will require interaction and communications with the component that owns that facility. On-site contractor personnel will comply with all component safety and security requirements. Any centralized systems administration operations in the vendor's proposal shall be performed in a contractor provided facility located at the discretion of the contractor. The contractor is responsible for the cost of connecting the remote facility to the administered system, and for the cost of maintaining that connection.

Contractor personnel co-located with RSC servers will provide active, hands-on support of the servers, as well as diagnostic support as needed. Supervision and management control of SA personnel remain with the contractor, CPMS will be responsible for program management. The contracting officer is responsible for contract administration and conflict resolution. At times, the RSC IT manager will provide guidance on systems administration activities. Two examples of appropriate component guidance are scheduling system downtime for maintenance and prioritization of data loads for user requests. Where system configuration and operations are concerned, the SAs will ensure that CPMS policy is followed, reporting any alternate requests or operations to the contractor operations officer and CPMS COTR.

The on-site SA will work a minimum eight hours per day (prime shift 8am to 5pm with 24 x 7 pager access for outages and performance degradation support). The SA shall respond to a page within one hour of notification. Pagers or cell phones will be provided as CFE. The host component is responsible for base support agreements for SAs assigned to overseas locations.

Local and remote systems administration tools will be left to the discretion of the contractor and are considered CFE.

Any local PC/LAN systems in the RSC will be maintained by component personnel and are outside the scope of responsibility of the contractor. Any client loads will be the responsibility of component personnel. Should an on-site SA assist the component on operational issues outside of the contract, the contractor will be responsible for correcting, at no charge to the Government, any hardware, software, or system issues caused by the SAs negligence.

C.3.1.2.4. Application Sustainment and Maintenance

Application sustainment and maintenance can be subdivided into three types of activities:

- Activity 1
  - Ensuring the smooth and error-free operations of DCPDS; and
  - Reacting to system outages or degradations in service caused by the application software to ensure that up-time expectations listed elsewhere are met.

Problem reports (PRs) are currently rated from level one (most serious) to level four (least serious). Level one PRs require immediate notification of contractor management to CPMS and are expected to be resolved within two days. Level two PRs require immediate notification if they occur during the workday. Level two PRs that are reported outside duty hours require notification to CPMS by 8:00 AM central time the next duty day. Level two PRs are to be resolved in a patch by the following week. Level three PRs require no special notification, must include a workaround and be repaired by the next quarterly patch. Level four PRs require no special notification and must be resolved by the second quarterly patch following the occurrence.

- Activity 2

    - Providing system enhancements desired or required by CPMS or a DoD component resulting from modified business practices or DoD component regulatory changes. These are processed as System Change Request (SCR) and approved by the DCPDS CCB;

    - Documenting all code, configuration, and version changes in the production environment;

    - Keeping all server application environments consistent with the same software versions and releases;

    - Modifying Oracle HR Federal functionality (which includes DoD unique requirements, as well as Federal requirements that are not met by the Oracle HR Federal product). The contractor shall work closely with Oracle Federal to ensure all required changes are made in a timely manner and do not conflict with other customizations;

    - Distributing, installing, and testing of software upgrades and changes to each RSC server;

    - Providing an environment for test and demonstration of DCPDS;

    - Installing replacement hardware of CFE and loading software for all CFE and GFE;

    - Integrating all systems changes into the operations baseline.

- Activity 3

    - Weekly changes for Change Request Transmittals (CRTs) which are code additions or changes resulting from a federal regulation DoD policy or other directed authority;

    - List of Values (LOVs) are updates made to existing value tables which usually require the addition of a new code with start date or end dating of an existing code that is no longer valid for use;

    - Pay table changes are required for every pay table in DCPDS. This normally requires the addition of the new table with a start date and the end dating of that pay table's previous version. In some cases the pay table must be edited when incorrect values have been entered, but this occurrence is rare;

    - Measures of quality for CRTs and SCRs include timeliness and accuracy of the deliverable, in accordance with agreed upon contractor delivery dates.

    - There is another group of CRTs that do require code changes. They are primarily caused by regulation changes made by DoD or other directing authorities. These are code changes beyond LOV and pay table updates and are more resource demanding. The contractor will inherit approximately 30 of this type of CRTs and there are approximately 35 new ones submitted each month; and

- CRTs are provided with a requested delivery date. Dates are subject to further discussion based on workload or resource requirements. The Government reserves the right to direct specific dates where necessary.

The vendor's proposal will provide sufficient resources to meet all of the sustainment requirements. To facilitate projection of contractor resource requirements, the Government estimates there are normally 15 to 20 new SCRs provided for each quarter's release. It is possible the number may increase, but the resource requirements for each change will decrease as major process requirements are replaced by fine-tuning efforts. This does not relieve the contractor from providing additional resources to meet growing requirements. It is not possible to identify the amount of work that may be necessary to fix a specific maintenance requirement; some are very quick, one-line code changes; others may be a four-week system modification.

The contractor will maintain the current number of PRs related to the system. It is anticipated that at contract award the PR level assigned to the contractor will be 50 PRs. The contractor will maintain or reduce this level. By the end of the first contract year, the contractor will maintain the operational PR level of at least 50 open operational PRs following a quarterly patch. Developmental PRs related to emerging functionality do not have a baseline target number.

The contractor shall provide:

- Periodic major upgrades/releases to Oracle HR Federal, Resumix, Oracle DBMS, HP UNIX operating system, and other management tools;

- Software patches/repairs as appropriate;

- Quarterly release of customized Oracle code (the contractor will patch changes at least once a quarter);

- Release of time-sensitive system changes within 15 days (for planning purposes, there is an average of only one time-sensitive change per month); and

- LOV updates and pay table updates. These are normally released weekly, but the contractor may be required to update within 48 hours of receipt from CPMS. For contractor workload planning purposes, there are an average of 60 LOV changes and 75 pay table changes per month, not including January when they spike up to 600 table changes. (LOVs and pay table updates are submitted with CRT control numbers, but the workload for these is almost always very limited and therefore is counted differently from the CRTs in the Activity 3 section above.) There are normally no more than two 48-hour requirements in a month. (This information is provided for planning purposes only and shall not be a limit on the Government's activity and if the workload requirements differ this shall not be the basis for an equitable adjustment unless there are increased workload requirements exceeding the estimates by at least 10 percent.)

The contractor shall support the rollout of these upgrades to each RSC server. Formalized software upgrade planning shall occur monthly with a contractor status report delivered to CPMS. Normally, component operations require at least 120 days advance notice for any significant software upgrade. The Government provides software upgrades as GFE for those packages listed in section C.3.3, and the contractor is responsible for installing the upgrades as part of the contract.

The contractor will maintain a website that provides DCPDS users with a complete and current source of DCPDS-related files. The site will include, at a minimum, files that relate to DCPDS patches, Resumix upgrades, and AutoRIF upgrades. Changes to this website will be coordinated with CPMS prior to release.

Major software enhancements may include:

- Upgrade to new Oracle application version;
- Installation of complementary software products (all applications associated with DCPDS unless precluded by contract);
- Upgrade to new Oracle DBMS version;
- Security patches;
- Upgrade to the HP UNIX operating system; and
- Modification to the baseline by contractor.

The Government has developed the DCPDS Patch Release Procedures and Approval Process (Attachment 5) to assist the vendor in understanding the workload associated with patch release. Patch documentation shall be written in terms that functional users will find clear and effective. The contractor will make use of the functional-technical translator labor category, provided by CPMS in solicitation Section G.5, to develop this documentation. Read-me documentation guidance and an example may be found in Attachment 6.

The contractor will interact with commercial software companies that provide DCPDS software and act in the best interests of CPMS and the Government. This includes logging problem reports (e.g., Technical Assistance Requests (TAR) for Oracle) with the technical support organizations in those companies and following up on those problem reports until satisfactorily resolved. The contractor will maintain currency on those software products through information sources such as Oracle's Metalink and Appsnet website, and other sources. The contractor acts in the best interest of the Government in relationships with other commercial providers and must maintain complete confidentiality and the highest ethical standards in these matters, as related to the performance of this contract. The Government maintains support agreements on GFE, and through that support provides appropriate upgrades.

Periodically, the application vendors provide new releases to their software. The contractor shall provide updates to any graphical user interface (GUI) required to support these new releases, along with installation instructions and documentation of any such changes. The contractor shall determine the method of software distribution, but CPMS recommends providing web or file transfer protocol (FTP) access.

Components are responsible for installation of the Personal Computer (PC) build at component locations. Because there is only one DCPDS (not separate component systems), all system enhancements must be approved by the Change Control Board (CCB). The contractor will serve in an advisory capacity to the CCB when appropriate. The CCB meets quarterly and includes Video Teleconference (VTC) capability. The CCB Charter is provided at Attachment 7.

C.3.1.2.4.1. PR, SCR, and CRT Tracking Capability

The contractor shall provide and maintain a PR/CRT/SCR tracking system(s) that will meet the following requirements:

- Include all PRs, CRTs, and SCRs, including those against the systems qualification test (SQT) environment;
- Provide unique tracking numbers for each PR, CRT and SCR;
- Allow CPMS, contractor and component access to the tracking system for view and update;
- Generate notification of actions to be taken;
- Generate standard and ad hoc reports;
- Allow attachments (documents, screenshot images, links) to specific PRs/CRTs/SCRs; and
- Provide a complete audit trail of actions taken or pending.

The tracking system will include adequate security (access control, user accounts and passwords). The current data is maintained in Mercury Test Director, Remedy, and Domino.

C.3.1.2.4.2. Contractor Support of CSUs

This section describes system-level operations, sustainment and maintenance requirements for the CSU databases, CSU application, and metadata layer software.

There are up to 24 production, testing, and training CSU databases. The single configuration database is written on Oracle RDBMS software (currently Oracle 9i, with a planned transition to Oracle 10g). The CSU databases are read-only extracts from respective RSC and CMIS/CMIS-R HR application databases. In many cases, a single CSU database server provides consolidated coverage to all the offices supported by an RSC.

Information from RSC servers is downloaded nightly and refreshed to each respective CSU database server within the RSC. In addition to supporting the CSU application, the CSU databases are used as reporting instances throughout DoD. The CSU databases are accessed through a variety of reporting tools, such as Discoverer, Business Objects, COGNOS, and Access, for processing a wide variety of queries and reports. Each CSU database requires ongoing system and database administration (DBA) support, including maintenance of system interfaces from the RSC server and DBA maintenance.

The CSU application is a web-based application that uses the read-only extract from the primary RSC and CMIS/CMIS-R HR databases of record containing records of civilian employees. It is used by managers and personnel specialists, to view data about a specific employee or to run reports covering a group of employees. There are currently 23 standard reports that reside in the CSU database. The CSU Desk Guide can be found at Attachment 8

The metadata layer is used to make selected data elements available to users for query and reports generation. The current reporting tool used is Oracle Discoverer. During FY 2005, the reporting tool will be transitioned from Discoverer to Business Objects.

Requirements for changes to the CSU databases, CSU application, and metadata layer will be processed through the existing change processes, such as System Change Requests, Change Request Transmittals, and problem reports. Required changes can be a result of regulatory or legislative changes, Oracle Federal or contractor recommended additions, deletions or changes to the HR database, or a system enhancement. It is anticipated that over the next several years, major changes to the CSU infrastructure will be required to support various OPM initiatives (e.g., Enterprise Human Resources Initiative (EHRI), HR Line of Business (L0B), the implementation of NSPS and planned Oracle Federal schema changes.

The contractor shall be responsible for the maintenance of all code related to the CSU databases, CSU application and the CSU metadata layer. The contractor shall be responsible for all normal systems administration duties related to the CSU server such as upgrades, backups, and restores. The contractor shall be responsible for applying any software upgrades required for CSU database operations in coordination with CPMS. The contractor will be responsible for implementing/incorporating all CSU changes.

The contractor shall be responsible for monitoring the overnight refresh process between the RSC server and the associated CSU database servers. The contractor will send completion notices or error notices immediately after the update process runs. These are to be sent to local (RSC and/or CSU) and component representatives and may be accomplished by email (script generation is allowed). The contractor shall be responsible for beginning restoration of the CSU database, at any location, within 24 hours of problem identification, regardless of the cause. There are no specific COOP requirements related to the CSU database, since total refreshes can be accomplished. The CSU database, CSU application, and metadata layer will be supported under established help desk procedures.

The contractor is responsible for documenting CSU database system changes and software maintenance require documentation. Soft copy transmission of documentation is acceptable. The contractor must be cognizant of the fact that many Components use the CSU database to feed their own query modules. As such, they are very interested in advance notice of CSU database changes since it means they may need to make changes to their own software. The contractor must understand the concern of the Components in providing adequate notice of changes. Documentation shall be provided at least 30 days prior to planned quarterly patch applications and at least 24 hours before a weekly or emergency patch is applied. The major Component interest is identification of data schema changes (specific system configuration changes). Documentation should contain identification of refresh and data extraction changes from DCPDS to the CSU database (table and column reference) and changes in field size. The contractor shall cross-reference and highlight DCPDS data element changes with CSU database elements to ensure CSU database integrity in any patch or release.

The contractor shall be responsible for maintaining the CSU Application User's Guide and updating it quarterly.

C.3.1.2.5. Contractor Support of Government Automated Staffing Tool

During the life of this contract, the contractor will support the current Government automated staffing tool, which is Resumix, or any replacement selected during this contract. The automated staffing is a Third Party tool; therefore, only partial support is required under this SOW. Under this SOW, the contractor is responsible for development and maintenance of interfaces flowing to and from DCPDS; database version updates, including loading of any patches or releases not strictly retained by the software vendor; system administration of the Government automated staffing tool database server to include the building of user identifications (IDs) as requested by the Component; and normal backup and administration called for by the software. The contractor is not responsible for database entries, system functional operations, or loading Resumix patches for the Components. The Government will be responsible for any Government automated staffing tool client loads at the RSCs.

C.3.1.2.6. Contractor Support of Centrally Managed Pay Tables

There are approximately 2,000 pay tables in DCPDS, with approximately 99 percent updated throughout the year with new salary values. The tables cover special salary tables authorized by the Office of Personnel Management (OPM), appropriated fund wage grade schedules, non-appropriated fund wage grade schedules, Title 38, agency unique tables, and tables required to process pay actions as a result of updating pay tables, i.e., local national constant tables, crosswalk payroll table, etc.

Each year, usually in January, a mass pay table update is required due to the lag time created by the Federal Appropriations Bill approval process. The mass table update process is time sensitive and has senior executive-level interest, as tables must be loaded to every agency/region to process a pay adjustment (pay increase) action for each employee. Pay adjustment actions cannot be processed until the pay tables are loaded. In the past, the tables have not been released on a known schedule, requiring quick reaction to load tables as soon as they are authorized. Despite these constraints, the contractor will produce timely updates to coincide with the first scheduled payout of the new calendar year; in this most critical and visible process.

In the annual table update process, some retroactive pay tables are updated twice during a three-month timeframe and some previously loaded tables require purging, as retroactively authorized tables supersede the tables. This requires special table update handling to insure tables are properly updated. Also, a table update for a short time frame may be required for a table that was end dated earlier (this means that the previous table is no longer authorized for use).

During the year, wage grade and other tables are updated. Tight timelines are the norm in processing these tables. Tables are usually provided to the contractor no later than Wednesday of a week with the requirement that tables be updated to production databases on Friday. At times, tables must be loaded to production databases within 48 hours of receipt by the contractor.

The contractor must accept tables in different formats, such as pipe delimited file format and excel text format. This requires the contractor to accommodate variations in how the software "reads" and loads the tables into DCPDS. The contractor will be required to load wage mariner tables, as these tables are usually updated in great numbers. The contractor must also load minimum/maximum and upper and lower boundary tables. Periodically, the contractor must establish a pay table that will result in opening salary fields in a Request for Personnel Action for manual salary input. This too, must be accomplished within a tight timeline, typically two days or less.

C.3.1.2.7. Automated Reduction In Force (AutoRIF)

AutoRIF is an HR processing application that uses data from DCPDS to simplify reduction in force (RIF) processing. AutoRIF develops RIF retention registers and tracks employee actions, qualification determinations, and actions updates. The application will report all employee changes relevant to RIF processing (position changes, seniority changes, etc.). Several features are available which allow flexibility while remaining within the RIF rules and regulations. AutoRIF has the capability to produce over 30 unique reports. AutoRIF is currently a stand-alone PC application that uses an Access 97 database. New functionality requirements will be required with the implementation of NSPS. The contractor shall be responsible for producing, maintaining and repairing the data extract between DCPDS and AutoRIF, and any code changes to AutoRIF.

The potential work associated with the integration of AutoRIF into the DCPDS baseline can be found at section C.3.5.5.

C.3.1.2.8. Technology Refresh

Technology refresh has two components. The first is to maintain GFE at optimal specifications. This includes the hardware associated with the corporate environment. The contractor is responsible for continually examining GFE to ensure the optimum configuration is applied to all such hardware and software. However, GFE used for testing the application may need to be at a lower than optimal level to simulate the configuration used in the field. The contractor will advise the Government of all GFE options available, provide sound analysis for upgrades, and schedule upgrades to minimally affect the performance of the testing program as well as the CMIS/CMIS-R. Upgrades should be applied to the corporate environment as soon as possible after approval.

Additionally, technology refresh includes the contractor actively researching commercial hardware and software alternatives that will improve performance, as well as fine-tuning any customized code to run more effectively and efficiently. The contractor will monitor performance and report to the Government on a monthly basis. During that period, the contractor will monitor hardware and software alternatives and provide the Government with recommendations quarterly. Recommendations should focus on changes that enhance the environment and are cost-effective. The contractor will provide the cost-benefit analysis information (at a high level) as part of any recommendations made. This evaluation includes determining the configurations required to support the RSCs and CSUs.

The contractor shall provide technology refresh recommendations. Government approval is required for all technology refresh changes and the Government reserves the right to fund technology refresh recommendations. As part of technology refresh, the contractor will maintain an asset inventory with a complete list of all GFE including RSC servers and server support software. The inventory will track and document the configuration details of each RSC server. The contractor shall provide a detailed quarterly report documenting this inventory to the CPMS COTR.

The contractor will manage the standards for the CFE, the associated inventory, and will research the technology that makes up the DCPDS. This will assist the contractor in performing other technology refresh activities.

The contractor will research the technology that makes up the DCPDS, and provide technical guidance, and planning support for technology refresh initiatives, including the actual specifications, purchases, and equipment installations. As part of technology refresh, the contractor shall participate as a non-voting member of the DCPDS Engineering Review Board (ERB), which reviews, approves, and recommends priorities for technical changes to the DCPDS hardware configuration, non-application software, and network connectivity. The contractor shall provide technical expertise on matters concerning system change design issues, release timing, software engineering, and related areas as set forth in this SOW. DCPDS equipment purchases are based on competitive bids in response to CPMS requirements. The contractor may compete as one of the bidders. The ERB charter (Attachment 9) provides more information on the ERB roles and responsibilities.

C.3.1.2.9. Value Engineering

Increasingly, private and Federal activities are encouraging their partners to use value-engineering techniques to improve quality and reduce costs. During the life cycle of this contract, there may be numerous opportunities for the contractor to submit proposals and accept additional requirements. It is anticipated that the contractor will utilize best practices as well as value engineering when preparing for and soliciting proposals to the Government. Therefore, the vendor will describe its value engineering program in this initial proposal, provide examples of other customers who have benefited from vendor value engineering efforts, and be prepared to discuss questions during oral presentations.

C.3.1.2.10. Base Technical Application

The DCPDS base application is Oracle HR Federal customized for DoD use. Based on the recent modifications, it has now been estimated that at least 25% of the operational code is unique customization that supports DoD business requirements. Each RSC server runs exactly the same customized version of Oracle HR Federal. The Government requires that standard software applications (operating and application software), e.g. Unix and Resumix, be used in conjunction with DCPDS. To the extent that different versions are being used, the contractor may be required to support several versions. The contractor is responsible for developing, implementing, and maintaining DoD unique customization, Oracle application configuration changes, and coordinating with Oracle to ensure resolution of problems with functionality that is generic to Government HR requirements under CPMS licensing contracts with Oracle. When Oracle is not able to provide a required system change in a timely fashion, CPMS may direct the contractor to make customized changes to DCPDS until the Oracle software is updated.

For the most part, all servers in the system are fully dedicated to software associated with the DCPDS. There are exceptions, mainly in the area of CSU database servers. In cases where servers are not dedicated, the contractor will remain in control of root authorities and share them only for specific Component tasks. Any additional use of system servers must be pre-authorized by CPMS with control exercised by the contractor. Unless stated, the Government is responsible for maintenance support on GFE software, including Oracle Silver Support.

C.3.1.2.11. CMIS/CMIS-R

Currently, the CMIS database server runs a suite of data management tools (including Oracle Discoverer Version 4.0 and Aris Noetix) and will receive transactions on individual records from the active RSC servers continuously via DTS or contractor provided solution. The feed is not required to be real-time. For example, it is expected that CMIS will be receiving data from RSC servers at all times. Should CMIS be taken off-line or be flooded with transactions (exceeding current bandwidth), transactions will be queued for transmission and replayed after CMIS is returned online.

There will be a limited number of users on CMIS, not expected to exceed 200 users (normally with fewer than 25 active concurrent users). The contractor shall be responsible for full CMIS system operations and systems administration and will build all required user IDs for CMIS, at the direction of CPMS. The contractor will have a resource person fully knowledgeable in data query to support the CMIS database. The Government estimates that one employee working half time will be required to develop and run specific system data queries.

The current CMIS will transition to CMIS-R in May 2005. CMIS-R is a data warehouse system that uses Business Objects as the standard query tool. It is estimated that CMIS-R will eventually support up to 300 concurrent users. The contractor shall be responsible for maintaining dual support of CMIS and CMIS-R until 30 days after delivery of the CMIS-CSU look-alike data mart.

C.3.1.2.12. Development and Test Environment

The vendor shall specify in its proposal, the technical environment required to operate, maintain, and sustain the development and test environment for all systems addressed in this document (e.g., DCPDS, CSU, Resumix, CMIS/CMIS-R). Unless listed as GFE elsewhere in this contract, the contractor shall provide all needed equipment to support this requirement. This includes all development, testing, change control, production control, and research and development applications, systems and equipment.

The contractor shall provide appropriate development, testing, maintenance of code library and other testing software. The contractor shall maintain a separate instance for testing with data records provided by the Government. The contractor must be able to refresh testing data, as needed, to ensure that clean data is tested.

At a minimum, the contractor will provide the following to support the development and test environment:

- Facility for testing. This facility does not have to be dedicated for this purpose; however, it is expected that a facility for testing will be needed approximately 60% of the time each year, declining to perhaps 40% by the last year of the contract. Access to the facility must be available to Government testers from at least 6am to 10pm local time and seven days a week during testing periods. Normal room climate controls shall be available during the testing period. Testing shall be the principal priority for this facility. The facility must be able to support testing on not more than a two-day notice.

- Full support of Resumix testing, to include server operations and any appropriate updates.

- Servers and peripherals with network access devices. This will include at least one high-speed printer specifically for testing.

- User and development workstations and software. The contractor shall provide a testing facility to house a minimum of 12 functional testers. This will include workstations that meet or exceed current system workstation minimums. The minimum screen size acceptable for monitors is 17”. The workstations must be able to be connected to multiple servers in the event of concurrent systems qualification and developmental testing.
- Mass Pay Test Environment**.** Testing will be accomplished in a stand-alone file server that allows for test system date alteration as well as a restricted-access database. The testing instance will be the primary site for year-round mass salary testing and will also provide the added benefit of Change in Appointing Office (CAO)/Transfer process testing. The test instance allows for system date alteration supporting date-specific processing and availability of a recovery copy of the database for reload, as needed. Multiple database reloads and mass salary executions to verify code modifications may be necessary. Testing will be conducted following load of draft or dummy pay tables that will not be incorporated into live environment table patches. Tables will be loaded within 24 hours of receipt, as testing time is normally very limited for pay adjustments. It is anticipated that the code level of this instance will be replicated in the contractor’s development test instance for their use. Normally, code patches will be maintained to match the current DCPDS SQT instance, with the exception of end-of-year (EOY) Oracle Federal patches and other mass pay adjustment related changes, such as pay calculation code modifications and new processes and procedures for calculation of pay fields. These exceptions will be loaded for early testing in the mass salary test instance. Routine scheduling of suspense, futures, AUTO-WGI, and

CAO Batch will be necessary to keep records current. Contractor systems administration (SA) staff will administer the routine batch jobs and CPMS (AMD) will be responsible for execution of mass pay, futures, batch print, etc. associated with actual mass pay testing.

- Network access and network access devices (LAN and connection into DISA DISN). Multiple testers will be accessing the development and testing instances from remote locations, which may include overseas locations. The contractor's solution must provide for such remote access. Access from the field user's workstation to the contractor's hub connection shall be the Government's responsibility; however, contractor support in identifying communication problems will be provided as needed. The contractor shall provide remote tester access through IP addresses and ensure connectivity maintenance. The contractor shall work directly with the Component/agency requesting remote access and CPMS System Management and Program Administration Branch to resolve firewall issues.

- Automated testing software, such as Mercury LoadRunner and Quick Test Professional, for application testing. This includes functional regression testing, system load and performance testing, or other automated application testing (several Mercury scripts have been developed for various types of application testing).

- Development and maintenance of automated testing scripts, such as those used by Quick Test Professional or Mercury LoadRunner, for conducting automated application or system testing.

- A uniquely identifiable application Problem Report (PR) system shall be available for all testing. The testing PR system and the operating PR tracking system may be jointly maintained on a single PR processing tool; however, the ability must exist for them to be reviewed and reported on separately. The PR system software must also be available to the remote testers so they may view the status of PR fixes and releases.

The location of multiple instances of the DCPDS application and database on GFE development and test servers will be at the discretion of the Government, with consideration of contractor recommendations and for systems performance. The addition of instances on these servers and subsequent maintenance is covered under this contract.

C.3.1.2.13. CPMS Training and Demonstration Servers and CSU Instance

These servers are located in Rosslyn, VA and support CPMS staff and system users training and for DCPDS demonstrations. The contractor shall support this environment to keep it current and functional with operational system releases. Other activities that are unique to these servers include refreshing databases in preparation for training classes and preparing the system for demonstrations (such as user IDs, and client set-ups), including the potential need to load beta and development versions of the DCPDS (loading of beta versions has not occurred during the past two years). Multiple instances (up to three) may be placed on these servers for training purposes. It is expected that day-to-day support requirements for the training and demonstration servers will be significantly less than for the RSC servers.

C.3.1.2.14. Public Key Enabling (PKE) Software and Software Maintenance

The contractor will provide PKE software on-going maintenance and upgrade support during the life of the contract. The contractor's PKE software solution shall ensure DCPDS interoperability with the DoD Common Access Card (CAC) and the Public Key Infrastructure (PKI) applications. This software will be used to validate user identities at sign-on as part of the web version of the DCPDS. PKE will operate as a part of the DoD CAC and PKI security programs. A PKE solution has been developed for both RSC and CSU users that has been certified by the Joint Interoperability and Testing Command (JITC). Additional information is provided at Attachment 14.

C.3.1.2.15. COREDOC

Because of the unique support requirements and the nature of related customized functionality, COREDOC is addressed separately in this SOW. COREDOC is a DCPDS application that provides position management and classification support. This DoD-developed application produces a single core document that integrates the position description; performance plan; cover sheet; and knowledge, skills, and abilities. COREDOC also interfaces with the Resumix application to exchange position and staffing data. It allows the electronic attachment and transmittal of core documents with the request for personnel action.

New or updated occupational series will also be coded and uploaded by the contractor as mandated by OPM. Because OPM is moving towards job family standards versus individual series standards, these changes could affect several occupational menus currently in COREDOC. The contractor will provide for functional testing of all COREDOC changes and updates prior to Government approval for implementation.

There are approximately 195 Standard Core Position Description menus (standard position descriptions not previously posted into series menus) in the standalone PC version that must be ported into the DCPDS. The contractor is responsible for determining the method for moving these documents from the PC version into DCPDS. When these menus are brought over, modification by users will be prohibited.

While COREDOC is the current automated classification tool employed by DoD, it is possible that CPMS may choose to explore other products that perform similar functions. In any case, the contractor shall provide support for a DoD automated classification program within DCPDS.

C.3.1.2.16 Developmental Testing

The contractor is responsible for ensuring that all developmental testing is accomplished prior to providing patches/changes to CPMS for functional testing. Initial developmental testing must ensure the specific fix has been completed (e.g., item has been added to an LOV) but this does not constitute full developmental testing. The contractor will run a baseline group of tests for every patch/change. The contractor will use Mercury Quick Test Professional or a similar tool that will allow a variety of different test scenarios to be run without tester intervention. For instance, each patch will have a test group of a set number of iterations of normal actions (e.g., position builds, appointments, 5XX and 7XX nature of actions, pay actions), regardless of the problems being patched or the functionality being added. This would provide a testing baseline and would ensure that no other process (e.g., position build) is broken when there is a patch to fix a Civilian Personnel Data File appointment edit. The contractor will perform a full range of developmental testing and prepare documentation prior to fielding any patch. Patch documentation shall be provided in language understandable to the functional user (see solicitation Section G.5).

C.3.1.2.17. Customer Support Unit (CSU)

The CSU, application and metadata layer are used to provide rapid query and report capability. There are currently 23 standard reports residing in the CSU. The term CSU database includes the CSU Oracle database; metadata layer (which makes selected data elements available to users) for reports generation; and standard reports. To allow for the tracking of personnel action processing, an events tracking module is data captured in the DCPDS events tracking module that is included in the CSU database to allow Components to collect performance data on personnel transaction processing. In most RSCs, a single CSU database server provides coverage for all of the CSUs supported by that RSC. A list of all CSU databases is at Attachment 2.

C.3.1.2.18. Disaster Recovery, Continuity of Operations, and Contingency Planning

The contractor shall provide disaster recovery, continuity of operations, and contingency planning support, including those for software applications, processed on various computer platforms, outlined elsewhere in this contract. Such support includes the capability to:

- Perform risk analysis;
- Develop disaster recovery and continuity of operations plans for contractors operations;
- Develop and conduct a disaster recovery exercise annually; and
- Recommend ways to increase the effectiveness of the plans and the continuity of service.

C.3.1.2.19. Intrusion Detection

The contractor shall:

- Provide intrusion detection support in accordance with the CPMS Intrusion Detection Policy and Procedures at Attachment 16; and
- Perform research on system vulnerabilities, conduct system penetration studies, and develop/obtain intrusion detection tools.

C.3.1.2.20. System Security Authorization Agreement (SSAA) Updates

On an annual basis, the contractor Information Assurance Officer (IAO) will review SSAA documentation and draft updates for CPMS review and approval.

C.3.1.2.21. System Certification and Re-Accreditation

The IAO will prepare a system risk assessment at least once every three years or whenever a risk assessment is warranted based on a proposed change in system operations. When a security test and evaluation (ST&E) is warranted, the IAO will prepare the appropriate test procedures and provide the ST&E test environment for the CPMS evaluation team. The IAO will document the findings in draft for CPMS review.

C.3.1.2.22. System Recovery Support Services

The contractor shall provide personnel resources to ensure a system recovery capability that will support Government goals and objectives. As a minimum, the contractor must provide the capability for hot-site/cold-site recovery of all critical software programs and sensitive Government information. The requirements for system recovery support services will be based on the analysis of the strengths and weaknesses of the system, as obtained through threat assessment and risk analyses and cost and benefit trade-offs. System recovery support services include the capabilities to:

- Detail and diagram hierarchical access and the storage system;
- Provide hot-site/cold-site system recovery support services that ensure continuity of operations for Government systems;
- Provide practical and effective interpretations of strategic planning for Government IT web-based systems as well as the alternatives available for system recovery;
- Provide or assess applicable feasibility studies for available system recovery support services alternatives;
- Provide alternatives for system recovery support services that are based on feasibility studies, best cost analysis, and requirements for continuity of IT operations; and
- Provide an off-site data vault service to provide a secure environment for critical system software and back-up programs and data and sensitive Government information.

C.. 3.1.2.23. Security Patch Updates

The contractor will ensure the timely issuance of security patches issued by the DoD Computer Emergency Response Team (CERT) to:

- Provide operational support for all applicable servers;
- Publish a program release describing the patches installed; and
- Maintain a monthly report on servers, security patches and dates installed.

C.3.1.2.24 Data Archives

The contractor shall generate and maintain a complete system archive every six months. The contractor shall generate and maintain a data archive every month. All of these archives shall be maintained during the period of this contract. Upon the last day of contractor activity, the contractor shall notify the CPMS COTR of the procedure to continue storage of the archived data for a period of two years, or shall transfer the data archive to the COTR. For either solution, the contract shall provide a method (software and/or necessary unique hardware) for the Government to review/recover the archived material. The format of the data backup and the storage media for the archive will be at contractor's option. The data archives and data therein are property of the Government and subject to non-disclosure requirements.

C.3.1.2.25. Additional Contractor Support

C.3.1.2.25.1. Additional Systems Administration and Maintenance on RSC Equipment

The Government may find it advantageous to allow the Components to utilize the contractor for systems administration and maintenance of HP UNIX or successor minicomputers located at the RSCs, in addition to the RSC server. Components will address these requirements to the COTR and they will be subject to COTR, CCB, and Contracting Officer approval. This might include utilization of the same network management tools and integrated backup, recovery, and COOP for such things as training or testing databases. Exercise of this optional work is at the sole discretion of the Government. The Government will provide the contractor a request for service with at least a 30-day advance notice. The request for service will include detailed requirements. The contractor will provide a proposal in response to the request for service, including proposed pricing. Following negotiations, if needed, and approval of the contractor's proposal, a contract modification will be issued for the agreed-to work at the agreed-to price. Absent unusual circumstances, it is anticipated that this will be issued on a firm fixed price basis.

C.3.1.2.25.2. Procurement Vehicle for Hardware and Software Purchases

During the performance of this contract, the contractor may be offered the opportunity to procure hardware and software for the Government in support of the contract. The Government will use fair and open competition for the procurement of DCPDS GFE hardware and software. The Government will use this vehicle when the contractor's proposal is most advantageous to the Government. For planning purposes, CPMS and the Components have procured millions of dollars of equipment to support this program in past years. It is expected that most current equipment will come due for life-cycle replacement at least once during the period of this contract.

C.3.1.2.25.3. Contractor Communications and Firewall Resolution Support

The contractor will be responsible for resolving communications and firewall problems related to DCPDS connectivity and operations at the RSC(s), CMIS/CMIS-R, and the development and testing environment. The contractor will log problems and work directly with DISA and local communications offices through resolution of communications and firewall problems. Resolution must be acceptable to CPMS. CPMS will serve as a conduit for communications with DISA and the users.

C.3.1.2.25.4. Contractor Assistance for Data Acquisition and Analysis

Until CMIS-R is deployed and stable, the contractor will continue to provide a designated staff member to respond to CPMS requirements for data queries for corporate level data. Data will continue to be extracted and compiled from the regional databases for corporate level data until it has been judged, jointly, by CPMS and the contractor that CMIS-R is, in fact, a reliable source of corporate data. The contractor will continue to provide, as needed, support for complex queries requiring table joins and multiple algorithms after CMIS-R is deployed.

C.3.1.3. Program and Project Management

C.3.1.3.1. CPMS Responsibilities

CPMS provides Government program management and overall coordination for the DCPDS effort including:

- Overall program management, including coordination of contractor support;
- Coordination with Component organizations;
- Ongoing management of performance metrics and DCPDS support requirements;
- Coordination of system development, testing, and roll out; and
- Chair of the CCB and the ERB.

C.3.1.3.2. Contractor Responsibilities

The contractor is responsible for performing the services in this SOW and shall provide an appropriate level of project and program management to meet those requirements and all performance metrics. The program and project management facility(ies) shall be provided by the contractor with staff offices located in San Antonio, TX.

The contractor project manager will meet bi-weekly with the CPMS COTR. The contractor shall provide a single point of contact (project manager or account executive). All contract issues shall be directed to the CPMS COTR and Defense Logistics Agency (DLA) Contracting Officer.

The contractor will provide quarterly performance reports on each of the performance metrics, along with a formal status report. These quarterly reports will show metrics by monthly performance. Performance metrics are shown in Attachment 10. Most metrics can receive a maximum score of 5 and a minimum score of 1. As long as the contractor scores at least a 3.75 average of its metrics scores, then additional on-site meetings are not necessary. If the contractor scores below 3.75, contractor reporting will change to weekly and the Government may initiate performance-based action.

The contractor is responsible for providing a fully qualified staff to perform duties under this SOW. Costs of personnel training, to include travel, are the contractor's responsibility and will not be reimbursed. However, if the Government changes its requirements, any related training and travel not already included in the contractor's training plan will be paid for by the Government in accordance with the cost reimbursement guidance in FAR Par 31; only direct costs will be reimbursed, and there will be no payment for profit, overhead, or indirect costs. Once training has been provided, the contractor is responsible for any costs related to maintaining these skills or for training replacement personnel.

The contractor will provide a mid-year and annual review for CPMS executive management. These meetings may be face-to-face or by VTC. The COTR and contractor project manager will coordinate time, place, method and material to be covered. The Government reserves the right to request additional on-site meetings with the contractor project manager or other contractor management team members as needed.

C.3.1.3.3. Optional Services

The following services constitute optional work, which may be exercised by the Government at its sole discretion. The procedures outlined in C.3.1.2.25.1 above will be applicable to the exercise of this optional work:

- Special projects (significant activities) the contractor can undertake to lower the cost of service or improve on performance metrics. The contractor will propose such activities to CPMS in advance and CPMS must agree to the changes prior to implementation. The Government reserves the right to fund special project recommendations. Examples of special projects are technology innovations, staffing changes, and facility and server consolidations.
- RSC hardware upgrade, installation, and replacement.
- End-user training documentation development, updates, and distribution. Functional system training and DCPDS User's Guide preparation are performed by CPMS and the using Components.
- Support of RSC server disaster recovery capability (COOP).
- Support of or work on component developed and supported systems that will interface with the DCPDS and conform to its application program interfaces.
- RSC resident LAN support activities.
- WAN management, however, the contractor is required to recognize and report WAN outages.

C.3.2. Interfaces

DCPDS provides data through a number of interfaces to other Departmental and external systems. There are also inbound interfaces providing information that is loaded into DCPDS. The number of these interfaces is expected to increase over the life of the contract and the contractor will develop these new interfaces under this SOW. Component-unique interfaces or new interfaces identified by the Government, which present an extreme workload increase, may be submitted by the Government as optional work, which will be exercised using the procedures outline in C.3.1.2.25.1 above. There is a list of current and projected interfaces that are covered by this SOW at Attachment 11. In most cases the work of generating these interfaces has already been automated and the contractor's role will be in scheduling, facilitating, monitoring and assuring that data transfer has occurred. Where the interface is shown as projected; when needed, the contractor shall build this interface and then maintain it for the remaining period of the contract. Problems related to data transmissions must be fixed by the contractor in accordance with Section C.3.1.2.4.

C.3.3. Government Furnished Equipment (GFE)

This section describes the equipment being provided to the contractor for the performance of this effort. GFE will be housed in a contractor facility, with the exception of the training and demonstration servers located at CPMS in Rosslyn, VA. Component GFE is located at RSCs or data centers supporting them.

A list of all GFE to be housed in the contractor facility(ies) is at Attachment 12. The Government will provide normal life-cycle replacement and/or major upgrades of GFE. The components have financial responsibility for upgrades, refreshes and replacement of the RSC and CSU processing environments and for facilities that are GFE. Should the Government add new work under this SOW, additional equipment shall be identified as a GFE or CFE responsibility during the modification process. The Government reserves all rights on applications and/or software loaded on GFE. All GFE will be used for the performance of the requirements of this SOW. This will be reviewed as part of a monthly performance review with CPMS staff.

The contractor will exercise normal property accountability procedures over CPMS GFE equipment to include property book control. The contractor may choose to place its own control labels on the GFE for this purpose. The contractor shall produce a quarterly report on the first day of the second month following each quarter (November, February, May and August) showing equipment under its control and indicating operational status and location.

The contractor shall place all GFE servers in a secure data center environment, certified by appropriate Government staff members. In the event the Government finds deficiencies, the contractor will take corrective actions within 90 days or move the servers into an approved data center with no loss in productivity and no additional expense to the Government.

The Government requires that all development and testing servers be located within the same LAN as the facility that houses the primary development staff and the testing facility.

When the contractor begins its efforts under this contract, the following will be in place as GFE:

- Regional servers and production processing environments, including local printers, peripherals, modems, and network access devices that will remain at the RSCs;
- End-user PCs, workstations, and LANs;
- WAN access via DISN between all existing locations, including a single contractor data center (unless multiple data centers are included in the proposal and accepted by the Government);
- LAN access within each Government site;
- CMIS/CMIS-R database, including all peripherals and network access devices located at the contractor's data center.
- Software licenses or proof of ownership of all business application software:
    - Business Objects
    - AutoRIF, version 3.3
    - Oracle HR Federal, version 11.5;
    - Oracle 11i Application Server;
    - Oracle Server – Enterprise Edition;
    - Oracle Workflow Cartridge;
    - Oracle Developer Server Cartridge;
    - Oracle Developer;
    - Oracle Designer;
    - Oracle Discoverer, version 4;
    - Oracle RDBMS, version 9i and 10g;
    - Oracle Advanced Security Option (ASO);
    - Oracle Self-Service;
    - Oracle Payroll;
    - Resumix, version 6.4.6;
    - Mercury Win Runner, LoadRunner, and Test Director, version 7;
    - Kintana Object Migrator;
    - Sterling Commerce Connect Mail;
    - MERANT, PVCS Manager, Tracker and Reporter;
    - HP UNIX, Windows new technology (NT) and Windows 2000 and related tools that are bundled with the server;
    - HP OpenView Internet Services
    - RMAN
    - Quick Test Professional;
    - TOAD;
    - Ultra Edit;
    - Executables or customized source code for all business applications; and
    - ETL software, the processing software that moves RSC data to the CMIS-R database.

The following will be provided as GFE on an as needed basis:

- RSC servers, including upgrades and replacements;
- Systems administrator workstations for contractor employees located at Government RSC sites;
- Ongoing maintenance of all software that was provided as GFE;
- Hardware maintenance, warranty and repair of all GFE;
- Upgrades for software provided with the initial equipment by the hardware contractor to the Government and provided as GFE; and
- All RSC and CPMS operational CSU database equipment and maintenance, including upgrades and replacements.

The Government intends to keep all GFE under warranty or maintenance for the duration of the project.

For those support services supplied at a Government facility (on-site), the Government will provide the necessary office space, office furniture, telephone, fax machine, and copier access.

C.3.4. Contractor Furnished Equipment (CFE)

C.3.4.1. Overview

The contractor shall provide all equipment (hardware, software and communications) and supplies necessary for ongoing contractor operations. This includes all support necessary for office operations, development activities and testing at the contractor's facility(ies).

The equipment and supplies will, at a minimum, include:

- Workstations, PCs, and printers;
- A data communications analysis tool;
- Automated server-monitoring tools;
- All telephone facilities, including costs for telephone calls to and from contractor facilities;
- WAN access via DISN between all contractor locations not approved at the time of contract award;
- Help desk tools (i.e., phones, a single worldwide help desk toll-free number, workstations, help desk software, call management tools, and call center monitoring tools);
- Systems management hardware and software tools (i.e., HP Openview, CA Unicenter, BMC Patrol, or Tivoli TME);
- DBA and data management, systems management, and project planning tools that are

specified by the contractor to meet or exceed the performance metrics (their selection is left to the discretion of the contractor with approval by CPMS);

- Data back-up utilities, tapes, and offsite storage costs (for CMIS and testing environment); and
- Development and test environment for Oracle applications and Resumix application or its replacement within the DCPDS (all software and network components) that might be required beyond that listed in GFE. Frequently, multiple instances of the Oracle application or Resumix application are necessary to allow for version upgrade testing.
- Any other equipment required to be provided by the contractor by any provision in this SOW but not listed above.

All CFE upgrades, refreshes, replacements, or software changes shall be at contractor cost. Changes in CFE, hardware or software, that may impact the DCPDS operation must be approved by CPMS. The contractor shall include a listing of all CFE as a separate section of the quarterly equipment inventory report. All costs for repairs and maintenance of CFE are the responsibility of the contractor.

C.3.4.2. Contractor Facilities

The contractor shall provide the staff, systems, management tools, and facilities to be used to supply requisite services. At a minimum, the contractor shall provide:

- Environmental controls including fire suppression;
- Utilities (including telephone capabilities, water, heating, ventilation and air conditioning);
- Network systems (i.e., patch panels, facilities access, LAN infrastructure, WAN infrastructure, and phone system);
- Power supplies, including an uninterrupted power supply, battery backup, and backup power generator on-site;
- Physical security and security-related hardware; and
- Emergency facility plans.

The contractor shall provide support service from a fully functional data center. The contractor should be able to accommodate facility growth of up to 20% during the period of the contract. CPMS reserves the right to enter and audit any contractor facility providing service under this SOW upon 48-hour notice. CPMS will cooperate with the contractor to protect any contractor trade secrets.

The Government requires that the contractor development activity be located in the vicinity of the CPMS system development functional staff, currently located in San Antonio, TX. The Government requires that the vendor specify in their proposal the development activity location and the setup of the development office. A part of the Government's evaluation of the vendor's proposal will be ease in access to the proposed development site. The contractor is responsible for all security and communications at the development site. The Government will provide access to the NIPRNET as well as a ".mil" account for use by the contractor. Government approval is required for the use of other communication solutions. The vendor may use other communication solutions to connect its offices provided the data remains secure. The contractor's use of non-Government provided communication solutions does not relieve the contractor from meeting all requirements of this SOW and the applicable performance metrics.

C.3.5. Future Developments

This information is provided to offer the contractor an understanding of future requirements that may arise related to this system. The types of services described elsewhere in this SOW and the services required to accomplish the requirements in the following sections may be added as optional work for each of these sections, at the Government's sole discretion, using the procedures in C.3.1.2.25.1.

C.3.5.1. National Security Personnel System (NSPS)

The National Defense Authorization Act for Fiscal Year (FY) 2004 enacted chapter 99 of Title 5, United States Code, "Department of Defense National Security Personnel System," which authorizes the Department of Defense (DoD) to establish a new human resources (HR) management system for the Department's over 800,000 civilians. NSPS will be a flexible and contemporary civilian personnel management system that will enable the Department to restructure the civilian workforce and allow it to establish a stronger correlation between pay and performance. NSPS will be the new HR management system for the DoD civilian workforce. The law allows the Department to establish new rules for how civilians are hired, assigned, compensated, promoted, and disciplined, within the framework of merit principles. With that authority, the Department will develop an HR management system that will attract, retain, reward, and grow a civilian workforce to meet the national security demands of the twenty-first century. Changes to DCPDS will be needed to accommodate new rules, regulations, and processes based on the design of NSPS, such as pay banding, pay for performance, new reduction-in-force (RIF) rules, new appointing authorities, and new kinds of personnel transactions, including conversion in and out. The design and implementation of NSPS will be conducted using a spiral development approach. Implementation of the first spiral currently is scheduled to occur in July 2005, and will include approximately 60,000 DoD employees (across Components, most likely General Schedule (GS)/General Manager (GM) and possibly existing demonstration projects or alternative personnel systems). Implementation of succeeding spirals will occur through FY 2007. The law authorizing NSPS does not prescribe the specific elements of the new system. The system will include a performance-based model. A new performance management system will be designed to ensure a closer link between pay and performance. NSPS will also bring new, more flexible and streamlined processes for recruiting and hiring, advancement, promotion, employee disciplinary appeals, and RIF.

The code modification required for NSPS will be added to the Defense Civilian Personnel Data System (DCPDS), which will continue to be the enterprise system for DoD civilian HR. The Civilian Personnel Management Service (CPMS) requires support for the modification of

DCPDS in order to convert DoD civilian employees to NSPS. This includes technical support for the design, development, testing, testing, deployment, and operation, sustainment and maintenance of system changes evolving from the NSPS civilian HR system. Work will include DCPDS software development; system operations, sustainment and maintenance during phased implementation; application management; configuration management; system and database administration; security; and all system integration functions currently performed by the contractor for the current DCPDS environment.

Software development, maintenance, and support of DCPDS must be tailored to support NSPS. The scope of these requirements includes software design, development, testing, deployment, maintenance, and integration. In sum, the requirement is to modify DCPDS to accommodate NSPS, including modification of existing software and development of new functionality. These efforts may include, but are not limited to:

- Provide solutions that will allow expansion of the NSPS framework in future phases beyond the first spiral.
- Integrate commercial off-the-shelf (COTS) software solutions, where available and appropriate.
- Include General Schedule (GS)/General Manager (GM) and possibly existing demonstration projects or alternative personnel systems.
- Integrate Oracle Federal support within the code development.
- Provide a separate development and testing environment to isolate NSPS code, which will be integrated into the current production environments upon successful completion of qualification and acceptance testing.
- Provide an automated Within Grade Increase (WGI) buy-in calculation capability to support the first spiral implementation in July 2005.
- Develop and deliver a mass employee and position "conversion in" process to support NSPS implementation. Note: While it is expected that the initial implementation will include only GS/GM employees (and possibly other demo employees or alternative personnel systems), there will be a requirement to develop conversion processes for other pay plans subject to NSPS, such as Federal Wage System employees.
- Develop code to support mass locality adjustment for delivery and implementation, subject to the final design of NSPS.
- Integrate a pay-for-performance module within DCPDS. This toolset will support the NSPS performance management system (e.g., defining and setting performance objectives, documenting a performance plan, inputting performance feedback, capturing and calculating scores, automating a "pay pool" process). This must include form/report development, requirements analysis, recommended alternative solutions, and integration into a comprehensive pay-for-performance module. A market study of existing COTS solutions may be required.
- System changes for conversion of employees into NSPS include code changes for Nature of Action, Legal Authority, Pay Plan, and use of Tenure Group I with veterans' recruitment appointment. The Government will provide these requirements as they are developed.
- The payroll interface that supports Defense-wide civilian pay, as well as other data feeds, must be modified to support NSPS required changes to DCPDS. These revisions will

include, at a minimum:

- Defense Civilian Pay System (DCPS) interface
- Resumix application
- Integrated Voice Recognition System/Employee Benefits Information System (IVRS/EBIS)
- AutoRIF
- COREDOC
- Central Personnel Data File (CPDF); Joint Processing and Adjudication System (JPAS); Defense Manpower Data Center (DMDC), to include Defense Eligibility and Entitlements System (DEERS) interfaces
- DCPDS Customer Support Unit (CSU) and Corporate Management Information System (CMIS)

In addition, the contractor will be responsible for specific software development and maintenance objectives and performance requirements, as follows:

- Analyze functional and technical requirements, design, develop, document, test, and qualify initial and updated releases that satisfy applicable requirements documentation.
- Develop, document, update and maintain interfaces between and among the existing and new components, in accordance with guidance provided by the Government, to facilitate integrated requirements planning with exchange of appropriate data.
- Provide a testing and training environment to support initial fielding of the NSPS application.
- Support all testing and integration necessary to achieve fielding and operational use.
- Update system documentation as directed by the Government to accommodate integration with other applicable DCPDS modules, and maintain interoperability within DCPDS and interface frameworks.

- Maintain DCPDS configuration management (CM) standards and processes throughout development, deployment, and operation, sustainment, and maintenance.

- Provide a scaleable, integrated product to deploy on a variety of hardware, as well as allow developers and Component customers to configure systems tailored to their specific needs.

- Provide capabilities for sharing and aggregating data/information for partial or complete plans, within, between and among the Components and agencies.

- Minimize life-cycle costs to develop, field, maintain, and evolve NSPS components while achieving end-user perception of a high-performance system.

- Meet or exceed functional and performance requirements as specified in the current DCPDS primary contract service level agreements (SLAs) (i.e., SLAs will apply to NSPS, where applicable).
- Meet Information Assurance and DoD security requirements.
- Adhere to DoD civilian HR operational, system, and technical architectural standards.
- Ensure consistency in integrating NSPS with DCPDS.
- Maintain design and coding standards in accordance with DCPDS current practices.

Software and hardware design objectives must include a plan for maximum use of COTS integration solutions to meet functional requirements for users, as appropriate.

C.3.5.2. Increase in Regional Operations

DoD is the prime user of the system. There are currently two additional non-DoD user agencies. There may be more non-DoD agencies that decide to use DCPDS. In response to this SOW, the vendor will provide proposed pricing for this potential future work (section L.1.3 provides the format for the proposal). The proposal should include the price for systems administration, deployment (to include two mock conversions), and database administration for small, medium, large and extra-large databases. Existing conversion code will be used by the contractor; however, some level of change to conversion code is normally required as each new agency is added. Agency specific system requirements (such as data items, interfaces or business rules) will be added as optional work using the procedures in C.3.1.2.25.1 prior to a new agency becoming a DCPDS user. For the purpose of sizing each of the RSCs, we identify them as small (considered fewer than 12,500 records); medium (over 12,500 but fewer than 30,000 records); large (over 30,000 but fewer than 60,000 records); and extra-large (over 60,000 records). A record is considered to be an active employee supported by the RSC or a non-employee user of the RSC system.

C.3.5.3. Decrease in Regional Operations

The Government expects that through the life of the contract there may be further changes in the numbers of RSCs operating in DoD. This may be caused by consolidation of RSC operations, closure of RSCs or consolidation of all Component RSCs into a single RSC. The overall work under this contract will decrease if such closures occur. Starting with the second month following the last action on a closed RSCs server, the pricing for regional operations support will be recalculated based on the RSC size (see section 3.5.2). The amounts bid by the vendor for section 3.5.2 for increased RSC operations will be used as the reduction amount should reductions occur.

C.3.5.4. Injury Compensation/Unemployment Compensation (IC/UC) System

The current IC/UC automated system is a stand-alone application that relies on data feeds from DCPDS and Department of Labor. The contractor would be responsible for developing and accommodating this module with DCPDS.

C.3.5.5. AutoRIF

The development work to bring this stand-alone product into DCPDS as an integrated module is possible future work. (See section C.3.1.2.7)

C.3.5.6. Database Purge and Archive Capability

CPMS is currently assessing the need to add archive and purge capability for the RSC databases. The requirement is to address the rapid growth of the databases, while maintaining the ability to provide ready access to historical data and to maintain the relational integrity of the data. The intent is to add this capability to the DCPDS technical environment. Should the Government request a proposal for this work, the contractor would be responsible for supporting and maintaining this capability. Any added software and hardware related to this capability will be provided as GFE.

C.3.5.7. Priority Placement Program (PPP)

The DoD PPP provides the DoD placement service for civilian employees who are displaced as the result of right-sizing and base closure initiatives. The PPP relies on a stand-alone automated system to register employees affected by RIF actions. The system matches vacancies with employees' skills. The benefits of integrating this system into the DCPDS include the elimination of the stand-alone application and increased efficiency in registering employees, identifying vacancies, and making employee placements. Should the Government request a proposal for this work, the contractor would be responsible for accommodating this module within the DCPDS.

C.3.5.8. Self-service

Oracle Self-Service (SS) provides employees, HR professionals, and supervisors the ability to access, view, and change HR data using a standard web browser. Access privileges and security set-up determine what the users see, and the selected fields that may be available to change. For example, individual employees are given the ability to update their personal addresses, while supervisors would not be allowed to do so for employees. By transferring the responsibility for updating data to the owner or administrator of the information, data accuracy is increased and administrative costs are reduced.

There will be many challenges associated with developing and deploying SS to employees, HR professionals and supervisors throughout DoD. Strategies for addressing these challenges are integral to managing the overall success of this project. Challenges and initiatives include, but are not limited to:

- SS provides functionality currently available in other applications (Employee Benefits Information System (EBIS), MyPay, and Thrift Savings Plan (TSP)) across DoD. In order to discontinue these highly effective programs and rely on SS functionality, CPMS must ensure that the SS version meets or exceeds existing functionality.
- Numerous levels of customization are possible within SS down to the desk-top level. CPMS must carefully define the types of customizations to allow and at what level they may be performed.
- The security hierarchy within SS is completely independent of the existing HR hierarchy. This means that, unless CPMS is able to leverage existing hierarchy structures within HR,

extensive development will be required to recreate existing hierarchal structures across DoD. This feature is basic to the control of employee and manager access, workflow routing, and any transactional approvals consummated in the system.

- A process does not exist at present in the SS module that easily provides for employee record movements from one organization to another, assignment of new supervisors to new employee record sets etc. Analysis will be required to ensure reassignments of employees within HR do not have to be replicated within SS.
- With the advent of Public Key Infrastructure (PKI) and the Common Access Card (CAC), research must be done to determine whether an employee will be able to access SS only from their PC at work, or whether there will be capability for employees to access from other than a .mil address.
- NSPS may necessitate enhancements to the SS module, particularly with respect to the appraisal capability and the Compensation WorkBench functionality. (Compensation WorkBench is the pay for performance module in the SS package.)

The contractor will be required to support CPMS in the assessment of SS functionality and technical capability as it relates to civilian HR. It is important to note that SS is an integral part of Oracle 11i and likely to be a key capability to achieve NSPS requirements.

CPMS owns Oracle licenses to support self-service functionality, with preliminary analysis underway to define a proposed self-service capability and supporting rollout schedule. The technical infrastructure (application, database, and supporting applications) must accommodate Self-Service implementation, upon determination of the features to be included to support DoD civilian HR. Should the Government request a proposal for this work, the contractor would be responsible for accommodating this functionality within DCPDS, to include evaluation, assessment, and recommendation for Self-Service implementation to optimize its use at the employee and manager levels. A detailed and comprehensive plan for rollout would be required.

C.3.5.9. Civilian Virtual In-Processing

Civilian Virtual In-processing (CVIP) is designed to assist in the hiring process by providing a web-based application that allows prospective employees the ability to complete required in-processing documents (identified by the HR staffing specialist) securely over the web. The information provided populates electronic in-processing forms and eliminates duplicate data entry by auto populating information on required forms based on the data collected. This application will support all aspects of employment in-processing, to include validating prospective employee eligibility, pre-appointment determinations, and appointment processing. CVIP also supports all new hires, regardless of recruitment source.

The majority of the information used to populate the forms are captured from two main sources: information provided by the potential employee over the web; and information captured from the Request for Personnel Action (RPA) in DCPDS.

The CVIP automated process enhances productivity, provides an audit trail, and moves the in-processing process into the electronic age. Should the government decide to implement CVIP, the Government will send the contractor a SOW, and request a proposal. If the Government agrees with the proposal and determines that the contractor's price is fair and reasonable, the Government will issue a contract modification authorizing the contractor to develop, implement, and maintain CVIP.

C.3.5.10. Integrated Staffing Suite

Results of a business case analysis (BCA) commissioned by CPMS and published in August 2004 indicate that the Department should continue efforts to implement an integrated staffing suite to be integrated with DCPDS. An integrated suite is defined as a suite of staffing applications, to include merit promotion rater, delegated examining unit rater, vacancy announcement builder, resume builder, applicant tools, referral certificate builder, web tools, and an archiving tool. A DoD enterprise solution would also accommodate the business process changes inherent in the implementation of the National Security Personnel System (NSPS). Should the Government decide to implement this functionality, the Government will send the contractor a SOW, and request a proposal. If the Government agrees with the proposal and determines that the contractor's price is fair and reasonable, the Government will issue a contract modification authorizing the contractor to develop, implement, and maintain this functionality.

C.3.5.11. e-Government HR initiatives

DoD has been engaged in several e-Government HR initiatives and may require the contractor to support the DoD plan for integration of these into HR business processes and the DCPDS architecture. These include e-Payroll, Enterprise Human Resources Integration (EHRI), e-Training, and Recruitment One-Stop. In addition, the Department has been a major contributor to the HR Line of Business (LoB) initiative, which may subsume the above-mentioned e-Gov initiatives. If DoD is named a Center of Excellence for HR LoB, there may be additional implementation requirements. Should the Government decide to implement this functionality, the Government will send the contractor a SOW, and request a proposal. If the Government agrees with the proposal and determines that the contractor's price is fair and reasonable, the Government will issue a contract modification authorizing the contractor to develop, implement, and maintain this functionality.

C.3.5.12. Unified DCPDS

To support a potential future DCPDS architecture, the contractor would be responsible for proposing the appropriate mix of hardware, software, communications, security, integration, and strategy for a single DCPDS database instance. Should the Government decide to implement a unified DCPDS architecture, the Government will send the contractor a SOW, and request a proposal. If the Government agrees with the proposal and determines that the contractor's price is fair and reasonable, the Government will issue a contract modification authorizing the contractor to develop, implement, and maintain this architecture. Pricing for regional operations support will be recalculated based on the RSC amounts bid by the vendor for section C3.5.2.

C.3.5.13. Integrated HR-Payroll

CPMS has prepared a business case analysis to support the Department's integration of HR and payroll by expanding the current enterprise DCPDS to include payroll functionality. Should the Government decide to implement this functionality, the Government will send the contractor a SOW, and request a proposal. If the Government agrees with the proposal and determines that the contractor's price is fair and reasonable, the Government will issue a contract modification authorizing the contractor to develop, implement, and maintain this functionality. The contractor would be responsible for producing and implementing a comprehensive technical plan for the hardware architecture, software development, testing, and implementation of this functionality.

C.3.5.14. COREDOC

With the advent of NSPS, the DCPDS COREDOC application will require major redesign. NSPS calls for a new classification structure, which includes career groups and pay banding, at the same time, simplifying the position description. This is a major deviation from the current system, which is based on pay plans and grades and lengthy position descriptions. The contractor shall provide support for any redesign to the DCPDS COREDOC application, to include functional testing and approval, as a result of NSPS implementation. Should the Government decide to implement this functionality, the Government will send the contractor a SOW, and request a proposal. If the Government agrees with the proposal and determines that the contractor's price is fair and reasonable, the Government will issue a contract modification authorizing the contractor to develop, implement, and maintain this additional functionality.

C.3.5.15. Additional Agencies

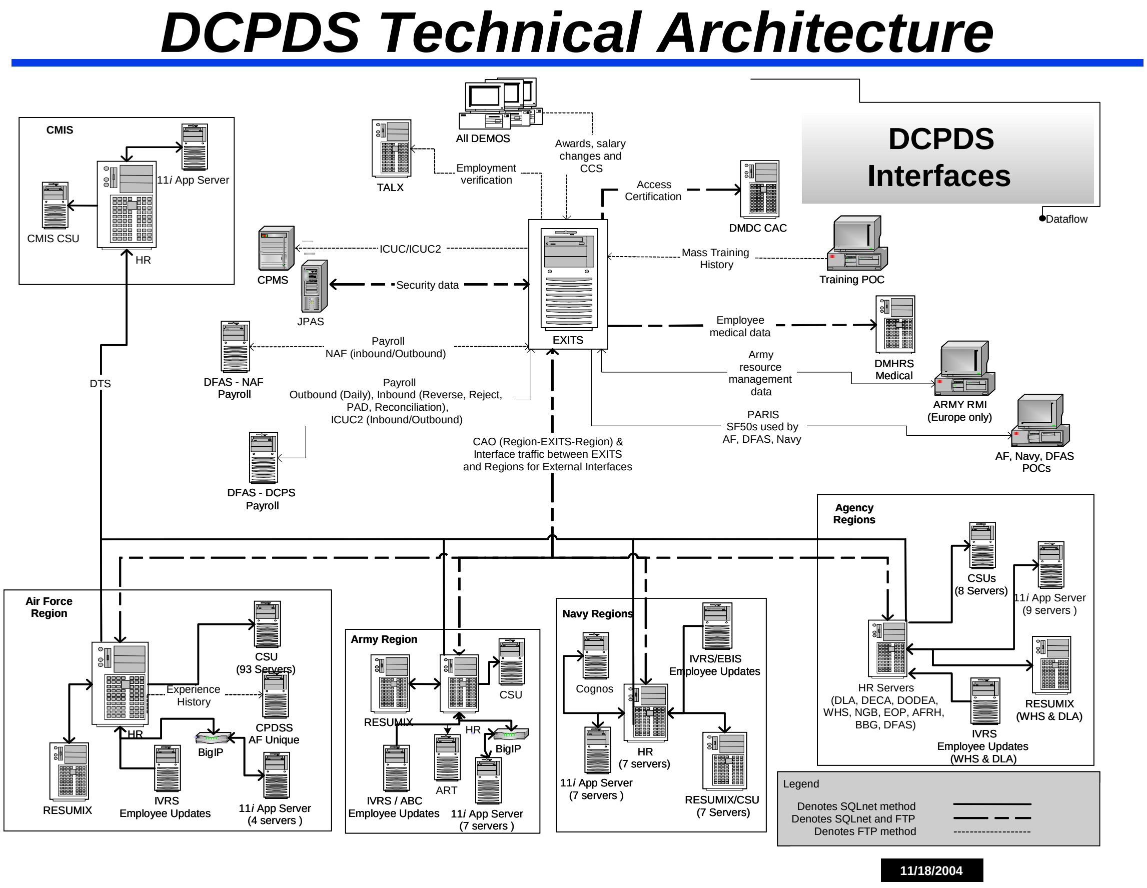
In the future additional agencies may become DCPDS users with technical configurations duplicating the RSCs. Should this occur, the contractor will be required to perform conversion and deployment of any added agencies as delineated in Section C.3.5.2. Configuration support for the added RSCs would be required. Attachment 3 provides a detailed description of the hardware and software located at each RSC.

C.3.6. DoD Component-unique DCPDS-related Work

Currently, six separate contract line numbers (CLINs) are for Component-unique tasks directly related to the DCPDS. These CLINs are funded by the respective Component; therefore, funding must be tracked separately. The Government expects that this functionality will continue under this contract. These requirements include, but are not limited to, operation of testing and training databases (systems maintenance to systems administration monitoring), specific program change warnings, added unique configuration changes (after CCB approval), and report and query support. The Government will send the contractor a SOW, and request a proposal. If the Government agrees with the proposal and determines that the contractor's price is fair and reasonable, the Government will issue a contract modification authorizing the contractor to develop, implement, and maintain this functionality.

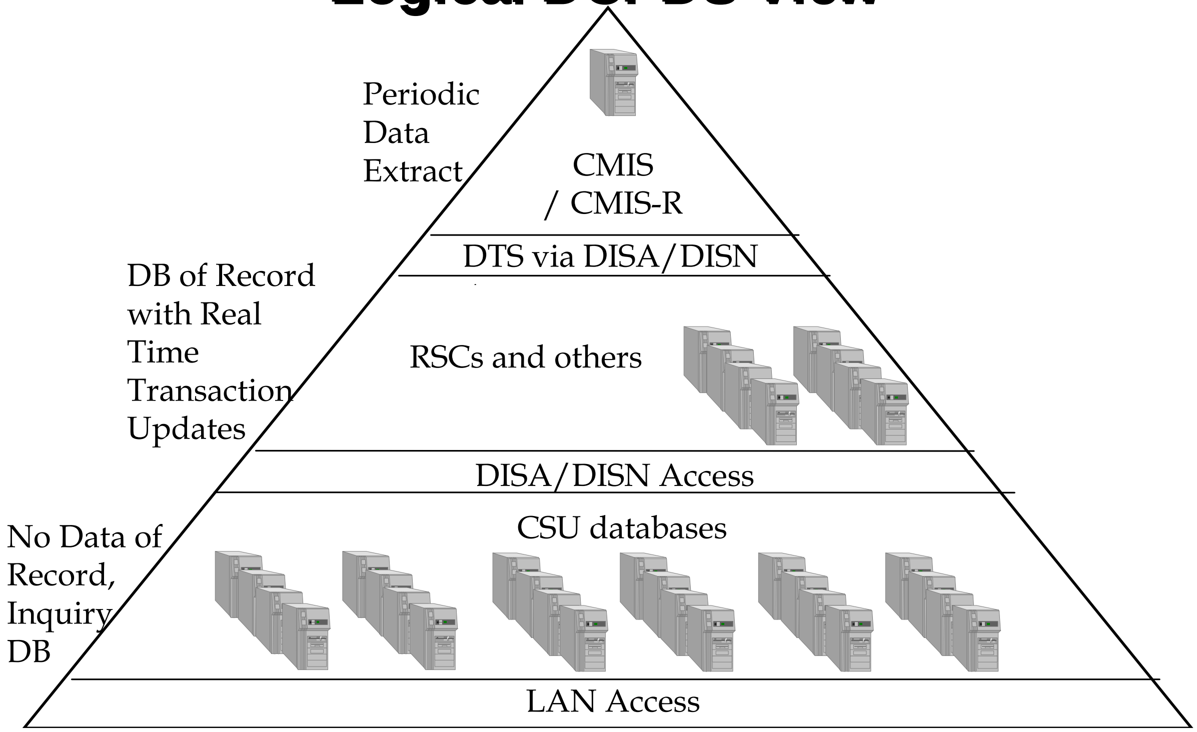
C.4. Technical Environment

The diagram, below, provides a high-level overview of the technical components of DCPDS. The shaded areas, the connection into the DISA DISN, and the support of the RSC servers, the CSU database servers, and CMIS/CMIS-R servers will be the responsibility of the contractor. The CPMS staff will oversee the contractor throughout this effort.



The diagram, below, depicts the flow of information and the method of network access into the system.

Logical DCPDS View



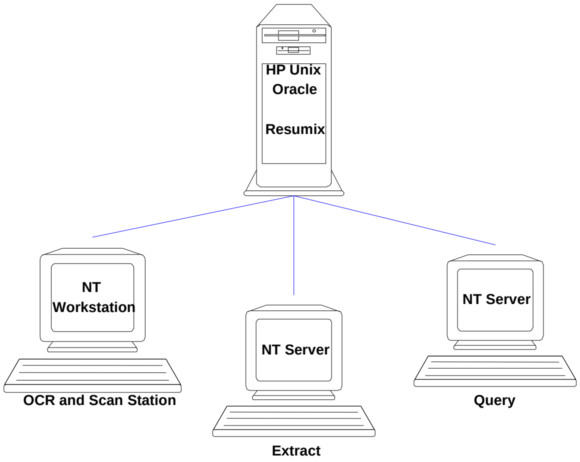
At the CSU database, information is accessed for inquiry purposes only. All transaction processing occurs at the RSC server level. Periodically, a subset of data is extracted from the individual RSC server and transmitted to the CMIS/CMIS-R database. The CMIS database is used for corporate-level analysis, reporting, tracking and trending. CMIS is housed on a suite of servers and storage devices. The current CMIS system is scheduled to be replaced by a revised version called CMIS-R. There is also a communications server in the total system configuration that moves data throughout the system (RSCs to CMIS, RSCs to payroll, payroll to RSCs). The databases at the RSCs contain the data of record.

DCPDS supports 22 DoD RSCs. At this time, there are two other non-DoD agencies using the system, the Executive Office of the President (EOP) and the Broadcasting Board of Governors and International Broadcasting Bureau (BBG/IBB). Currently BBG/IBB is sharing servers located with the Department of Defense Education Activity RSC; EOP is using a server located at the Washington Headquarters Services (WHS) RSC. For CSU operations, EOP and WHS are sharing one server, but with individual instances. For RSC operations, EOP and WHS have separate servers.

C.4.1. Architecture at RSCs

The contractor is responsible for recommending RSC hardware and configuration for optimal RSC operations; however, the Components are responsible for procurement and maintenance. The current technical plan specifies four dedicated Hewlett Packard (HP) servers for each RSC or agency supported. One is running HP-UNIX with Web server and application server combination, one is running HP-UNIX as the Oracle database server, one is running HP-UNIX as the Resumix application and database server, and one is running HP-UNIX as the CSU application and database server. The storage solution in use in the RSCs vary from HP-12H AutoRaids, HP-VA-7100, HP-DS-2100, HP-XP256, HP-XP512, HP-XP1024, Net Applications Network Attached Storage (NAS) Devices, and HP-VA7400. In some cases the RSC will also have three Windows NT servers supporting the Resumix application. The current CMIS environment consists of one HP-16-Way Superdome, one HP 9000 interface server, and one HP 9000 series query server. The CMIS-R environment will consist of on HP-16-Way Superdome database and replication server, one HP 9000 web and application server, and one HP 9000 Halfdome database and application server.

There will be approximately 181 HP-UNIX servers and 90 Windows NT servers that need to be managed. Windows NT servers are oversized and configured under a single domain to support the Resumix application. The configuration resembles:



The RSC servers do not communicate with each other (data are not shared between these servers) unless an employee record is transferred from one RSC to another. When this occurs, the data will flow through a central communications server, a part of the supported system. Attachment 13 provides the technical specifications for Resumix server configurations.

C.4.2. Web, Application, Database, CMIS, and CSU Servers

The system hardware configuration consists of HP UNIX 9000 series database servers, which vary in class from L2000s to Superdomes, and HP UNIX 9000 series Application / Web servers, which may range from L3000s to Superdomes. Various storage media are being used ranging from HP-SureStore 2100s to Net Application NAS devices and HP–XP256, XP512 and XP1024 Storage Area Network devices. Individual site configurations are provided in Attachment 3.

System software consists of: Oracle HR Federal 11i, Oracle RDBMS, Oracle Advanced Security Option, Resumix, Windows NT, Windows 2000, and related tools bundled with the servers. A complete list is provided in section C.3.3. A partial summary of application servers is provided below:

- Approximately 181 HP-UNIX 11 operating systems with LAN and WAN access;
- Approximately 90 Windows NT operating systems to support Resumix with LAN/WAN access;
- Communication ports; and
- Over-sized servers (anticipates new users and added functionality).

C.4.3. User Workstations

User workstations are Intel Pentium II or better, running Windows 98, Windows 2000, Windows XP, or Windows NT. Generally, the workstations are part of a LAN. Additional individuals may access each server via a WAN configuration. The contractor may make recommendations on RSC user workstations; however, the Components are responsible for ensuring that user workstations support the Oracle HR web-based application (DCPDS) and web-enabled CSU.

Under Oracle HR Federal 11i, users access the DCPDS Oracle application using Internet Explorer or Netscape over a secure Internet connection (https). The same applies to web-enabled CSU. Users will apply all additional and necessary products, such as the J-initiator, to facilitate access to these applications. The contractor will ensure these products are available to all users.

Users will ensure workstations can connect to servers after being provided the required configuration information supplied by the contractor. The contractor will assist users in resolving connectivity issues between workstations and applicable servers.

C.5. Performance

C.5.1. Overview

The contractor is responsible for providing solutions for work described in section C.3 of this SOW. As this is a turnkey solution for the operation, maintenance, and sustainment of the DCPDS, the overall outcome is a functioning and current system with adequate assets to keep it operating.

C.5.2. Performance Metrics

Performance metrics are critical to CPMS for the effective operation of the DCPDS. CPMS has developed a series of performance metrics that will be used to monitor the success of the contractor in performing the activities described in this contract. Some metrics are qualitative in nature and will be evaluated on a monthly basis. Some metrics are quantitative and will typically be measured daily, but reported and analyzed on a monthly basis.

The contractor shall provide services that meet or exceed the performance metrics shown in Attachment 10. The attachment delineates the initial performance metrics measured and managed as part of this SOW. While the stated performance metrics are not the only criteria to guarantee satisfactory performance by the contractor, they do represent the data the contractor will be required to collect and report.

Changes and updates to the performance metrics may be made with joint and mutual agreement between CPMS and contractor program managers.

To ensure that required services and support are provided in accordance with the performance metrics, the contractor is required to provide metric-based performance reports on a monthly, weekly, and daily basis as required by CPMS (see section C.5.4 below). The contractor will finalize the format and content of the reporting requirements for CPMS approval within 120 days of contract award. Reporting begins with the contractor's assumption of responsibilities on September 29, 2005.

C.5.3. Financial Impact of Performance Metrics

There are no financial performance incentives in this contract, but performance will be evaluated and reported in past performance evaluations, and reports, and will be assessed for purposes of contract administration, including option exercise. Should the contractor's overall performance fall below a 3.75 level (see performance matrix at Attachment 10), corrective steps will be requested by the Government. Should the contractor's performance not reach the 3.75 level following an improvement period that shall not exceed two months, financial disincentives will be applied. The Government plan for disincentives shall be:

- A 10% reduction in the monthly payment under the affected CLINs if the rating is from 3.74 to 3.50;

- A 15% reduction in the monthly payment of the affected CLINs if the rating is from 3.49 to 3.25; and

- A 20% reduction in the monthly payment of the affected CLINs if the rating falls below 3.25.

The Government invites the vendor to propose an alternate financial disincentive plan in their proposal, which will receive consideration.

In the event the contractor does not satisfactorily field the application of a patch to the DCPDS or any of its functional applications, the contractor will be assessed a .5 percent reduction in the monthly payment under the affected CLIN. The disincentive will be assessed against the current contractor invoice. This disincentive applies only if the Government has previously approved a patch release and the contractor fails to properly apply the entire patch to any production server. This does not cover situations where the approved code was erroneous.

Financial disincentives will not restrict the Government from also initiating action to terminate the contract for failure to perform. The Government retains the right to request corrective action on any work considered to be failing, regardless of the overall average.

C.5.4. Reporting Requirements

The contractor will provide daily, monthly, quarterly, and annual reports as discussed below. Reports must be in a meaningful and understandable format.

- The contractor is required to report on the following by October 15, 2005, and then annually or semi-annually as shown in section F: Certification of Help Desk Production Capability; Systems Administration Certification; Application Sustainment and Maintenance Production Capability; Performance Monitoring; and Technology Refresh Production Capability. The reports will follow a standard template of the contractor’s design and identify all new activity for each reporting period.

- Daily reports are required on system status that will culminate in a monthly and quarterly rollup.

- Monthly reports will include statistics for system uptime, identify the cause for any downtime (communications network, operating system, database, or hardware problems), and detail the actual downtime for each instance. The report must detail scheduled outages and reflect the RSC or RSCs affected. Reports must also include software and application performance reviews, which may require contractor sponsored monthly meetings for evaluation.

- The contractor will prepare and deliver a quarterly report on the status of security clearances for all contractor employees whose duties require they be automated data processing category I or II certified.

- The contractor shall provide a quarterly report on all GFE/CFE. The report will list all equipment, the operational status, applications on each server and the equipment’s location.

- The contractor will produce a quarterly performance metrics report. The report will break out performance results for each month and roll up quarterly scoring. The contractor will not produce the data behind the ratings, but will produce any and all related data if required by the Government.

- The contractor will maintain and make available all collected help desk statistics as mutually agreed by CPMS and the contractor.

- The contractor will provide an annual inventory assessment of the DCPDS infrastructure, including recommendations for improving DCPDS operations.
- The contractor will provide an annual report to the Director, CPMS. The annual report will be briefed at the annual review. The report will feature a roll up of all reports and activity for the previous fiscal year.

Additional reports may be required by CPMS and shall be provided by the contractor. There are also system-generated reports that the contractor will be responsible for supporting. These are normally CPMS requested data query (many have been designed), scheduled and run against the appropriate server(s). Completed reports are normally sent by electronic means to one or more locations. Few, if any, will require hard copy. Most new reports will be added to a library so that they may be reutilized. On average, six new reports are requested each year. For planning purposes, these reports are estimated to take 20 hours of development time each. Reports may be either direct structured query language or Oracle HR Federal reports.

C.6. Place of Performance

Performance under this contract must be in the continental United States to facilitate the required interface with the DoD HR functional community, the majority of which is in the continental United States. The contractor's corporate operation must be in the continental United States. Contractor facilities will maintain security standards and environmental controls that comply with commercial best practices (e.g., dual power and network feeds, raised floor, fire suppression etc.). The contractor is required to house the primary development work in a facility that is on the same LAN connection as the development and testing servers. The testing facility must be collocated with the developers and on the same LAN connection as the test server.

Within 90 days of contract award, the contractor shall establish a list of all contractor facilities being used, along with point of contact information. CPMS shall be provided access to this list online.

Travel will be required in the performance of this SOW. CPMS and the contractor are expected to work together to minimize travel expenses. Reimbursement to the contractor for travel shall be limited to the Government per diem rate, in accordance with the DoD Civilian Personnel, Volume 2, Joint Travel Regulations (JTR), Chapter 4, Part J (available at www.dtic.mil/perdiem/jtr.pdf). The location of contractor facilities could play a large role in determining the frequency and cost of travel. Estimated travel costs are to be included in the vendor's cost proposal. Contractor personnel will travel only with the approval of the COTR or his/her designated representative and related expenses will be treated as other direct costs (ODC). (See Travel Policy and Approval Procedures at Attachment 15.) Under no circumstances will the Government pay for first class or business class travel unless expressly approved in advance by the Government under circumstances that would allow first class/business class travel under the JTR (for example, required because of disability or medical reasons validated by competent medical authority).

Travel estimates in the vendor's accepted proposal will be set aside by the Government for the purpose of reimbursing actual travel. This amount is not considered part of the firm, fixed-price contract and does not accrue to the contractor unless/until travel is performed.

For vendor planning purposes or use in generating its proposal the history of non-deployment travel is approximately $60,000 per quarter. This includes required management travel, systems administrator developmental and local vicinity travel, and coordinating meetings.

C.7. Period of Performance/Contract Type

The contract performance period is for one year plus four option years. Unless indicated elsewhere in this SOW, the contractor is to start performing on September 29, 2005. This contract is a firm, fixed-price contract and time and materials. There is also a cost breakout for added work or decreased server requirements shown in the futures portion (sections C.3.5.2 and C.3.5.3) of this SOW. In the event that additional work is placed against this contract, whether they are firm, fixed price or time and material efforts, the primary work shall be performed and will not be affected by any additional tasks performed under separate modifications. While it is understood that some cross-utilization of personnel between requirements will be needed, the contractor will maintain sufficient staff to satisfactorily fulfill performance requirements necessary to support the primary effort. In short, additional staff will be provided by the contractor for additional, subsequent effort and the Government can request current breakouts and assignments of all contractor employees at any time. Work on the primary contract may not suffer due to additional work.

From time to time, during the period of performance of this contract, new task and subtask assignments will be issued. The Government may ask for a rough order of magnitude (ROM), based on new system or separate scope of work requirements. The Government expects receipt of ROMs within 2 weeks of request. Based on the nature of the specific requirement, the modification may be firm fixed-price or time and materials. Examples of the tasks or subtasks include purchase of: hardware, software, installation, integration, systems development, systems engineering, and systems support. Specific details of work assignments, deliverables, documentation, training, and applicable governmental standards will be provided in individual modifications to the contract. In addition, the requirements under the T&M CLINs are optional work and are not fully defined. As these efforts are further defined and ordered, they will be added to the contract by modification and in accordance with the guidelines in Section G of the solicitation.

C.8. Information Assurance Support Services

Authority for DCPDS System Access is controlled by the contractor in compliance with DoD Policy regarding protection of identity and information. Contractor personnel are required to sign a DCPDS Account Form - ID of Accounts and Information. All subcontractors are required to sign a non-disclosure agreement with the contractor.

CPMS maintains a robust Information Assurance (IA) program to support DCPDS. The contractor IAO, under the direction of the DCPDS Information Assurance Manager (IAM), assists in ensuring compliance with DoD IA standards and processes, including the most current

IA implementation regulations, DoD 8500.2, dated February 6, 2003. Contractor responsibilities in the area of information assurance include active participation in managing the certification and accreditation process for DCPDS, including the DCPDS SSAA; monitoring and reporting intrusion attempts or incidents; monitoring vulnerabilities, including all alert mechanisms used by DoD (i.e., IAVA, OSAs); and providing IA awareness training to contractor and other staff.

In addition, CPMS maintains an independent security consultant that participates in DCPDS IA processes and ensures the execution of DCPDS IA activities in accordance with the most current Federal and DoD laws and regulations aimed at IA compliance.

C.8.1. Information Assurance Officer (IAO)

The contractor will establish a security unit headed by a certified IAO to support DCPDS security policies and procedures. Security responsibility covers system assets under contractor control, including computer hardware, software, data, networks, documentation, physical infrastructure, and system access by contractor and sub-contractor personnel. Security policies and procedures are addressed in DoD Instruction 5200.40, dated December 30, 1997, DoD Information Technology Security Certification and Accreditation Process (located at website www.dtic.mil/whs/directives/), DoD Directive 8500.2, February 6, 2003, Security Requirements for Automated Information Systems (located at website www.dtic.mil/whs/directives/), and the DCPDS System Security Authorization Agreement (SSAA), dated September 29, 2004.

The IAO will ensure that contractor facilities adhere to system security policies and procedures provided in the SSAA. The IAO will participate in CPMS security visits to contractor sites in order to determine security worthiness for site certification. The IAO will ensure contractor sites have implemented corrective actions identified from the site visits. Security unit facility shall be contractor provided and the location is at the discretion of the contractor.

The IAO will maintain appropriate password controls for contractor and sub-contractor personnel as described in the SSAA. The IAO will implement procedures to handle and store system data in accordance with the Privacy Act of 1974 and as “For Official Use Only” as required in the SSAA.

The vendor will submit an additional labor category for this position. The document will show the expected work, skills of the incumbent as well as education and experience. The document is to be submitted with the vendor’s proposal, as outlined in section L.1.2.7.

C.8.2. Automated Information Security Support

The contractor shall provide operational and analytical security support for information assets. Such support includes the capability to:

- Provide support necessary to evaluate the integrity of operating systems and environments;
- Provide operational and analytical support of security system software;
- Ensure the operation of trusted computer systems consistent with the SSAA;
- Support full compliance with the DoD Instruction and Directive cited above;

- Ensure that users, both internal and external, are not unreasonably affected by the operation and administration of security system software; and
- Provide independent operational and risk assessments of security administration and implementation.

C.8.3. Computer Security Awareness and Training

In accordance with DoD Directives, the IAO will ensure that contractor and sub-contractor personnel are provided appropriate security awareness training prior to accessing the DCPDS and on an annual basis, thereafter, as described in the SSAA.

C.9. Government Furnished Information (GFI)

The Government shall provide GFI as required to perform the tasks described in this SOW. This GFI is expected to include, but is not limited to:

- Estimated transaction volume;
- Civilian personnel information;
- Human resources policy information;
- Human resources special projects information;
- Oracle HR system specifications; and
- DCPDS infrastructure specifications.

Unless otherwise specified, all GFI will be treated as CLOSE HOLD - FOR OFFICIAL USE ONLY. GFI shall not be duplicated, distributed, published, or disclosed without the express written consent of the proper Government signing authority. DoD owns the DCPDS and any intellectual property rights associated with the DCPDS. It is understood that the contractor may bring intellectual property to the project during performance of tasks. The Government shall honor contractor intellectual property rights as appropriate.

The contractor shall generate and maintain a complete system archive every six months. The contractor shall generate and maintain a data archive every month. All of these archives shall be maintained during the period of this contract. Upon the last day of contractor activity, the contractor shall notify the CPMS COTR of the procedure to continue storage of the archived data for a period of two years, or shall transfer the data archive to the COTR. For either solution, the contract shall provide a method (software and/or necessary unique hardware) for the Government to review/recover the archived material. The format of the data backup and the storage media for the archive will be at contractor’s option.